IN THE UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WISCONSIN

ECOLAB, INC., and NALCO)
COMPANY, LLC, d/b/a NALCO)
WATER, an ECOLAB COMPANY)
and/or NALCO WATER,)
)
Plaintiffs,)
)
-vs-) No. 3-cv-102-wmc
)
JESSICA GRAILER,)
)
Defendant.)

The deposition of LAURENCE D. LIEB, called by the Defendant for examination, pursuant to notice and pursuant to the Federal Rules of Civil Procedure for the United States District Courts pertaining to the taking of depositions, taken before Noreen E. Resendez, Registered Professional Reporter and Notary Public within and for the County of DuPage and State of Illinois, at 300 North LaSalle Street, Suite 4000, Chicago, Illinois, commencing at the hour of 9:11 a.m. on Tuesday, January 23, 2024.

Page 2

A P P E A R A N C E S:

FAEGRE DRINKER BIDDLE & REATH, By
MR. DAVID YOSHIMURA
801 Grand Avenue, 33rd Floor
Des Moines, Iowa 50309
515.248.9000
david.yoshimura@faegredrinker.com

On behalf of the Plaintiff;

QUARLES & BRADY, LLP, By
MR. MATTHEW SPLITEK
33 East Main Street, Suite 900
Madison, Wisconsin 53703
608.251.5000
matthew.splitek@quarles.com

and

QUARLES & BRADY, LLP, By
MS. LAUREN BOLCAR
2020 K Street NW, Suite 400
Washington, DC 20006
202.372.9600
lauren.bolcar@quarles.com

On behalf of the Defendant.

ALSO PRESENT:
Christopher Messer - Videographer

Page 3

I N D E X

E X H I B I T S

LAURENCE D. LIEB

Page 4

THE VIDEOGRAPHER: We are now on the record. Today's date is January 23rd, 2024. The time is approximately 9:11 a.m. This is the video recorded deposition of Laurence Lieb in the matter of Ecolab, et al., versus Jessica Grailer heard before the United States District Court, Western District of Wisconsin, Case Number 3.23 CV 00102.

My name is Christopher Messer. I am the videographer.

At this time, Counsel, you may now state your appearances for the record and then our court reporter will swear in the witness.

MR. YOSHIMURA: David Yoshimura on behalf of plaintiffs with Faegre Drinker Biddle & Reath.

MR. SPLITEK: Matt Splitek of Quarles & Brady for the defendant. And with me I also have Lauren Bolcar, Quarles & Brady.

(Witness duly sworn remotely.)

WHEREUPON:

LAURENCE D. LIEB,

called as a witness herein, having been first duly

Page 5

sworn, was examined and testified as follows:

EXAMINATION

BY MR. SPLITEK:

Q. Good morning.

A. Good morning.

Q. How many times have you been deposed before?

A. I believe it's at least eight.

Q. You've done this before then but I'll go over some of the ground rules. You're under oath testifying just like you were in court.

Do you understand?

A. I do.

Q. The court reporter will need verbal answers and words so that the record is clear.

You understand that?

A. I do.

Q. If you don't understand a question, will you tell me?

A. I will.

Q. If you need a question repeated, can you tell me or the court reporter?

A. I will.

Q. All right. Also if you want a break,

Page 6

tell me that, too, please.

A. Absolutely.

Q. Who engaged you for this matter?

A. I was engaged by Ecolab Corporation through their original outside counsel, Fisher and Phillips.

Q. And when were you engaged?

A. I was engaged -- my recollection is early 2023.

Q. Do you remember when you were first contacted about anything relating to Jessica Grailer?

A. I don't recall the specific date.

Q. Was it right around the time you were engaged?

A. I'm not sure I understand the question.

Q. Were you -- did a lot of time elapse between when you were first contacted about anything related to Jessica Grailer and when you were engaged? Was there a gap?

A. I don't believe so.

Q. Okay. Do you remember when you first performed any work relating to Jessica Grailer?

A. My recollection is February or March of

Page 7

2023.

Q. All right. Other than this case, how many times has Ecolab or Nalco Company engaged you or your company, Tyger Forensics?

MR. YOSHIMURA: Objection to scope.

BY THE WITNESS:

A. I'm currently engaged on, including the Grailer matter, four matters.

Q. Those are current?

A. Current.

Q. Other than the four current Ecolab lab matters, have you ever been engaged on any other Ecolab or Nalco matters?

A. No.

MR. YOSHIMURA: Objection to scope.

BY MR. SPLITEK:

Q. Let's go through the four engagements. So one of them is this one, the Jessica Grailer engagement?

A. Yes.

Q. Do the other three also involve former Ecolab employees?

MR. YOSHIMURA: Objection; scope.

Page 8

BY THE WITNESS:

A. Two do and one I believe involves -- well, all three do and current employees as well.

Q. Okay. What was the first matter where you were engaged by Ecolab?

MR. YOSHIMURA: Objection.

BY THE WITNESS:

A. I believe it was Ecolab Nalco versus Anthony Ridley and Chem Tree.

Q. Okay. And where is that case pending?

MR. YOSHIMURA: Objection.

BY THE WITNESS:

A. I believe it's pending in federal court in Tennessee.

Q. Okay.

A. I could be wrong.

Q. All right. And that case involves an employee or former employee named Anthony Ridley, right?

MR. YOSHIMURA: Objection.

BY THE WITNESS:

A. That is correct.

Q. When was the second case for which Ecolab engaged you?

Page 9

MR. YOSHIMURA: Objection.

BY THE WITNESS:

A. I believe it is a case involving a former employee of Ecolab named Simon Walker.

Q. Where is that case pending?

MR. YOSHIMURA: Objection.

BY THE WITNESS:

A. I don't recall.

Q. And what was the third case for which Ecolab engaged you?

MR. YOSHIMURA: Objection.

BY THE WITNESS:

A. I believe it is the Jessica Grailer matter.

Q. And what was the fourth case for which Ecolab engaged you?

MR. YOSHIMURA: Objection.

BY THE WITNESS:

A. It's -- I believe the case caption is Ecolab versus Washing Systems, Inc.

Q. Okay. And Ecolab versus Washing Systems, Inc., does that involve any Ecolab employees or former employees?

MR. YOSHIMURA: Objection.

Page 10

BY THE WITNESS:

A. It does.

Q. How many employees or former employees?

MR. YOSHIMURA: Objection.

BY THE WITNESS:

A. One former employee.

Q. And what's that former employee's name?

MR. YOSHIMURA: Objection.

BY THE WITNESS:

A. I believe his last name is Shanklin.

Q. Can you spell that for the record?

A. I can. S-H-A-N-K-L-I-N.

Q. All right. And is Chem Tree involved at all in that Washing Systems, Inc., matter?

A. I don't believe so.

MR. YOSHIMURA: Objection.

BY MR. SPLITEK:

Q. Does the Washing Systems, Inc. matter involve any question as to whether anyone exfiltrated materials from Ecolab or Nalco?

MR. YOSHIMURA: Objection. And at this point, I think now that we're getting into the substance of these cases, Counsel, and we may be approaching questions of matters that

Page 11

are attorney-client privilege, I'm going to instruct the witness to the extent that any of his answers may be privileged, that he not answer this question.

BY THE WITNESS:

A. I'm not attorney but my understanding of the question you're asking would ask me to reveal potentially privileged information.

Q. Okay. And that's fine. I just want to make sure the record is clear.

You are on -- well, for both of you -- your attorney's instruction you won't -- you can't tell me whether in the Washing Systems, Inc. case, you performed any analysis of whether somebody exfiltrated materials from Ecolab or Nalco?

A. My understanding of the question is you're asking me to reveal or disclose privileged communication I had with Ecolab's counsel.

Q. All right. How did you first get connected with Ecolab?

A. I was engaged by their outside counsel, Fisher and Phillips.

Q. Did you know anyone at Ecolab or Nalco before you were first engaged by Ecolab?

Page 12

A. I did not.

Q. All right. All together, about how much have you been paid or has your company Tyger Forensics been paid for Ecolab engagements?

MR. YOSHIMURA: Objection.

BY THE WITNESS:

A. I would -- my recollection is roughly $100,000, in that neighborhood.

Q. How many times has the Fisher Phillips law firm engaged you or your company Tyger Forensics?

MR. YOSHIMURA: Objection. I'm not sure answering that question would disclose any sort of privilege. I may have been engaged by them on matters that were internal investigations of that sort. So I don't know -- I don't want to breach any sort of confidentiality.

BY MR. SPLITEK:

Q. I'm just asking for a number. How many times?

A. I don't recall.

Q. Can you estimate it?

A. No.

Page 13

Q. Is it more than 20?

A. I don't recall.

Q. Is it more than 50?

A. No.

Q. Is it possibly between 20 and 50 times?

A. No.

Q. Is it under 20?

MR. YOSHIMURA: Objection; asked and answered.

BY THE WITNESS:

A. I don't want to disclose any sort of -- or breach any sort of confidentiality agreements.

Q. All right. And just so the record is clear, you're not going to tell me how many times the Fisher Phillips law firm has engaged you?

MR. YOSHIMURA: Objection.

BY THE WITNESS:

A. No.

Q. How did you first get connected with Fisher Phillips?

A. I was brought in by another electronic discovery provider to -- because I'm a licensed Michigan private investigator, which is required to perform computer forensics in the State of

Page 14

Michigan, and this other E-discovery provider did not have a licensed Michigan PI on staff, and that case involved Fisher Phillips.

Q. And when was that?

A. Two years ago.

Q. Did you know anyone at the Fisher Phillips firm before you were first engaged by Fisher Phillips?

A. I had never heard of them before that.

Q. What were you asked to do when you were initially engaged for this matter?

MR. YOSHIMURA: Objection to the extent that question calls for privileged communications with counsel, instructing the witness not to answer.

BY THE WITNESS:

A. Can you be more specific, please?

Q. First I want to get an answer at least to the question I asked.

So when you were first engaged for this matter, what were you initially asked to do?

MR. YOSHIMURA: So to the extent that your answer would call for a privileged communication between you and Fisher

Page 15

Phillips, don't answer that. If you can answer the question without revealing privileged communication, answer it.

BY THE WITNESS:

A. Well, I can state for the record that I created a forensic image of Jessica Grailer's former work laptop. I then built forensic databases of that laptop using Magnet Forensics Axiom and Passmark's OSForensics software tools. Performed forensic analysis, wrote my declaration, which you obviously have a copy of.

Q. And I'm just going to ask it again, though.

When you were initially engaged for the matter, what were you asked to do?

MR. YOSHIMURA: Same objection. Also asked and answered.

BY THE WITNESS:

A. I really don't understand ur question.

Q. And just to clarify, I'm not asking what you did. I'm asking what you were asked to do.

MR. YOSHIMURA: Same objections and same instructions.

Page 16

BY THE WITNESS:

A. Yeah, I honestly don't understand your question. I honestly don't. Can you please be more specific what you're ...

Q. Did you talk to a person when you were engaged for the matter?

A. Yes.

Q. And who was the person?

A. That was Michael Honeycutt at Fisher and Phillips.

Q. And did Michael Honeycutt and you talk about what you were being asked to do in the engagement for which you were being engaged?

MR. YOSHIMURA: Objection. To the extent that question can be understood to call for privileged communications, I'll instruct Mr. Lieb not to answer.

To the extent you can answer without revealing privileged communication, you may.

BY THE WITNESS:

A. Yeah, I don't understand what you're -- can you please be more specific in what you're asking me. I really don't understand your

Page 17

question.

MR. SPLITEK: Can you read the question back again, please?

(Whereupon, the record was read as requested.)

BY THE WITNESS:

A. It sounds -- I'm interpreting your question that you are asking me to reveal potentially privileged communication.

Q. To make sure the record is clear then, you're not going to answer the question, right?

MR. YOSHIMURA: Objection.

BY THE WITNESS:

A. Are you asking me to reveal privileged communication?

Q. No. Right now I'm asking just for you to confirm that you're not going to answer the question.

MR. YOSHIMURA: Objection.

BY THE WITNESS:

A. So please be more specific in your question so that I'm not being asked to reveal privileged communication with Fisher Phillips counsel.

Page 18

Q. So my current question is just whether or not you are going to answer the last question. That's all. It's nothing about Fisher Phillips right now.

MR. YOSHIMURA: Objection.

BY THE WITNESS:

A. Well, my current understanding is you're asking me to directly reveal privileged communication or potentially privileged communication with Ecolab counsel.

Q. And so for that reason you're not going to answer the question, right?

MR. YOSHIMURA: Objection; asked and answered.

BY THE WITNESS:

A. Yes, I'm not going to reveal potentially privileged communication.

Q. Thank you. I just want to make sure the record is clear as we're moving through here.

And if you're not going to answer this question, just tell me. But what were you told this case was about when you were first engaged?

MR. YOSHIMURA: Objection. To the extent this calls for privileged

Page 19

communication, I would instruct Mr. Lieb not to answer.

BY THE WITNESS:

A. I don't recall being told the case -- you're asking me what the case was about. I don't recall any conversation about what the case was about.

Q. Have you invoiced your client for the work you've performed in this matter?

A. I have.

Q. And have your invoices provided itemized time entries for your work?

A. They have.

MR. SPLITEK: I'm going to hand you Exhibit 1.

(Deposition Exhibit No. 1 was introduced to the witness.)

BY MR. SPLITEK:

Q. Is Exhibit 1 a copy of your first invoice in connection with this matter?

A. I believe so.

MR. SPLITEK: I'm going to hand you Exhibit 2.

Page 20

(Deposition Exhibit No. 2 was introduced to the witness.)

BY MR. SPLITEK:

Q. Is Exhibit 2 a copy of your report in this matter?

A. Let me read it. It is.

MR. SPLITEK: I'm going to hand you Exhibit 3.

(Deposition Exhibit No. 3 was introduced to the witness.)

BY MR. SPLITEK:

Q. Does Exhibit 3 contain the exhibits to your report in this matter?

MR. YOSHIMURA: While he's reviewing this matter, I would just move the final exhibit in the packet that you've just handed me appears to have been cropped in the margins of the pages so it may not reflect the complete exhibit.

BY THE WITNESS:

A. Yeah, that's right. If we're going to refer to the exhibits, particularly the ones from OSForensics, which are in full color --

MR. SPLITEK: Can we go off the record

Page 21

one moment?

THE VIDEOGRAPHER: The time is 9:30 a.m. We are going off the record.

(Whereupon, a discussion was had off the record.)

THE VIDEOGRAPHER: The time is 9:32 a.m. We are back on the record.

BY MR. SPLITEK:

Q. Mr. Lieb, I am handing you a new and better copy of Exhibit 3.

A. Okay.

Q. Does Exhibit 3 contain the exhibits to your report in this matter?

A. It does.

Q. So does Exhibit 2, which is your report, contain a complete statement of all of the opinions you will express in this matter?

MR. YOSHIMURA: Objection.

BY THE WITNESS:

A. I don't really understand that question.

Q. All right. Well, I'll ask it again. It's just yes or no.

Does Exhibit 2, which is your report,

Page 22

contain a complete statement of all of the opinions you will express in this matter?

MR. YOSHIMURA: Objection.

BY THE WITNESS:

A. I guess it depends on what questions you ask me. So if you ask me about the report, then I'll answer regarding my opinions expressed in the report. But if you're asking me a question about an opinion or information unrelated to what is in this report, then I'm going to answer you directly.

Did I misinterpret your question?

Q. Let's try again.

Does Exhibit 2 contain a complete statement of all of the opinions you currently intend to express in this matter?

MR. YOSHIMURA: Objection.

BY THE WITNESS:

A. I don't want to answer a question that I think you're asking me because occasionally that gets people angry with me. So do you want me to answer what I think you're asking me or should I give you a chance to ask more specifics or ...

Q. Why don't we start with you answering

Page 23

the question that I asked.

A. Okay.

Q. So what's that?

A. Please repeat it.

MR. SPLITEK: Can you repeat the question for the witness?

(Whereupon, the record was read as requested.)

BY THE WITNESS:

A. I'm not really understanding that question. But I will answer that the -- I stand by, and no information, no evidence has come to my attention or knowledge that has changed any of the conclusions or opinions I reached or expressed in my declaration. And if you ask me a question that was not covered in this subject, I'm going to answer you directly as well.

Q. Does Exhibit 2, which again, is your report, contain a complete statement of the basis and reasons for the opinions that you intend to express in this matter?

MR. YOSHIMURA: Objection.

BY THE WITNESS:

A. I honestly don't understand that

Page 24

question. So I will respond that -- no information has come to my attention that changes any of the opinions expressed in my Exhibit 2 report. But if you ask me a question that -- on a subject that was not covered in here, my understanding is I'm required to -- you are an officer of the court, I'm required to and I will answer you directly.

Q. So taken together, do Exhibits 2 and 3 identify all of the facts and data that you considered in forming your opinions in this matter?

MR. YOSHIMURA: Objection.

BY THE WITNESS:

A. Yes.

Q. And taken together, do Exhibits 2 and 3 identify all of your relevant qualifications?

A. Yes. I'm not trying to be difficult. I'm honestly not understanding the question.

Q. You considered a Digital Guardian report in your analysis, right?

A. I did.

Q. And Digital Guardian is software that Ecolab had installed on Grailer's work laptop,

Page 25

right?

A. Yes. To be specific, Digital Guardian is a software that is running on a server controlled by Ecolab and there's an agent, what is known as an agent, running on all Ecolab employee's work stations, the Digital Guardian.

So there is both. There's the overall software running on a server and then there's an agent that's running on all the Ecolab employees' laptops.

Q. And the Digital Guardian agent was running on Grailer's laptop, right?

A. Yes.

Q. Okay. And Digital Guardian is designed to record the exfiltration of files, right?

A. That's my understanding. According to Digital Guardian's website it categorizes itself as a data loss prevention software.

Q. For example, Digital Guardian is designed to make a record if files are copied to an external storage device like a USB thumb drive, right?

A. That is correct.

Q. Okay. And in your report, you opine

Page 26

that Grailer copied files to a USB thumb drive, right?

A. I do.

Q. Okay. Does the Digital Guardian report that you considered record Grailer copying those files to her USB thumb drive?

A. No, because it cuts off at a time before those acts occurred.

Q. What time does it cut off?

A. I don't have the report in front of me so I don't recall specifically.

Q. Did you do any analysis to determine that the Digital Guardian report cut off at a certain time?

A. If you're asking me if I analyzed the Digital Guardian report that was provided to me by Ecolab, I did analyze that report.

Q. And that was a bad question. So let me ask a better one.

How did you determine -- well, let me back up one more time.

You said the Digital Guardian report cut off at a certain time, right?

A. Yes.

Page 27

Q. What do you mean by it cut off?

A. The -- I don't have the Digital Guardian report in front of me, but it's -- the last entry is a specific time and that's what I'm -- that time is what I'm describing is the end of that report on January 8th.

Q. Okay. Do you know whether the Digital Guardian agent was still running on Grailer's laptop after the last entry in the Digital Guardian report?

A. I don't know.

Q. Did you do any analysis to figure out whether it was continuing to run after the last entry in the Digital Guardian report?

A. I did not.

Q. But you could do that, right?

A. I could do it if I was asked to, yes.

Q. But you didn't do it?

A. I didn't do it.

MR. YOSHIMURA: Objection.

BY MR. SPLITEK:

Q. And I take it no one did ask you to analyze whether the Digital Guardian agent was continuing to run in Grailer's laptop after the

Page 28

last entry that you saw in the Digital Guardian report?

MR. YOSHIMURA: Objection to the extent that may call for privileged information. I would instruct Mr. Lieb not to reveal any privileged communications.

BY THE WITNESS:

A. Yeah, I received no direction whatsoever from Ecolab's counsel as to what type of analysis to perform. I performed -- since theft of trade secrets is -- one of our practice is my specialties. I have a standard set of analysis steps that I undertake in each of these cases. So I performed those steps in this case as well.

BY MR. SPLITEK:

Q. But sitting here today, you don't know whether or not the Digital Guardian agent was still running on Grailer's laptop after the last entry that you saw in the Digital Guardian report?

MR. YOSHIMURA: Objection; asked and answered.

BY THE WITNESS:

A. I did not perform any analysis to see

Page 29

if the Digital Guardian agent running was still running after the Digital Guardian report that was provided to me that Ecolab had ended.

Q. And if you didn't perform any analysis to see if it was running, then you don't know whether it was running, right?

MR. YOSHIMURA: Objection; asked and answered.

BY THE WITNESS:

A. Yeah, I didn't analyze it because I didn't need to.

Q. What do you mean you didn't need to?

A. Well, in my Exhibit 2 declaration all of the -- so first let me state for the record that I'm an independent expert, meaning no matter who asks me a question, my answer is going to be exactly the same, period, end of story.

Literally 100 percent of my work is based upon science and can be replicated by a qualified peer. And I've been taught and mentored that to the extent that -- to assume that judge, jury, officers of the court are all brilliant in their own field, to the extent they don't understand my answer, it's a failure on my part to

Page 30

explain my opinion in plain English.

So the items I'm expressing in Exhibit 2, I quote and reference, you'll notice there is footnotes where I found the evidence that I'm referencing in my declaration and you'll see that I reference a specific location on her laptop computer, for example, so that any qualified peer can go look at a forensic image of her laptop, the same exact location that I found, and they would find that same exact evidence.

Q. So right now I want to keep talking about the Digital Guardian report.

A. Okay.

Q. So the Digital Guardian report was -- Digital Guardian was designed to record the type of exfiltration that you're accusing Grailer of engaging in on January 8th, right?

MR. YOSHIMURA: Objection; argumentative.

BY THE WITNESS:

A. My understanding working with Ecolab and their Digital Guardian reports on multiple cases is that Ecolab has -- and with any company using Digital Guardian, will set up rules such

Page 31

that if a rule is violated, it's -- a flag is triggered. But that's kept at the -- on the, we'll call it the server side.

So the local agent running on the machine is just a local agent that's reporting back or sending information to the Digital Guardian server.

Q. Do you know whether or not the Digital Guardian report records any instances of Grailer copying files to the USB thumb drive that you mention in your report?

A. I did not -- my analysis of the Digital Guardian report provided to me by Ecolab did not find any evidence of, what I would describe as exfiltration of files to an external USB media or I would have referenced that in my report.

Q. But don't you want to know why the alleged exfiltration was not recorded in the Digital Guardian report?

MR. YOSHIMURA: Objection.

BY THE WITNESS:

A. Well, the exfiltration that I found was performed after the Digital Guardian report cuts off time-wise. So that is the explanation.

Page 32

Q. But you already told me that you don't know whether the agent was still running.

A. You're not understanding -- so there is an agent.

MR. YOSHIMURA: He has to ask you a question then you can answer the question. There is no question pending right now. That was a statement from counsel.

THE WITNESS: Sorry.

BY MR. SPLITEK:

Q. My next question is what were you about to tell me?

MR. YOSHIMURA: Objection.

BY THE WITNESS:

A. Can you repeat your statement because you were --

Q. Yes.

My statement was you told me earlier that you don't know whether the Digital Guardian agent was still running on her laptop after the last entry that you saw on the report, right?

A. Right.

Q. And then you said you don't understand, right?

Page 33

A. I don't understand what?

MR. YOSHIMURA: Objection.

BY THE WITNESS:

A. I understand --

Q. I think you told me that I didn't understand.

A. Well, you were mischaracterizing. So the --

MR. YOSHIMURA: Larry, he did not ask you a question.

THE WITNESS: Okay, sorry.

BY MR. SPLITEK:

Q. My question is what were you going to tell me that I didn't understand?

MR. YOSHIMURA: Objection.

BY THE WITNESS:

A. The Digital Guardian agent running on the Ecolab employee machines sends information to the Digital Guardian server and then that is what -- from what the reports are run, including the one that I analyzed.

Q. How would Grailer have exfiltrated the files that you say she exfiltrated without that being recorded by Digital Guardian?

Page 34

A. I see that as she may not have been connected to the Internet. That's my explanation because she -- again, the agent running on the machine has to report -- on her laptop has to report back to the Digital Guardian mother ship.

So if it is -- if it is not connected or she shuts off that agent, it is not going to report back. So the Digital Guardian mother ship is only reporting and providing -- collecting information that the laptops are sending to it.

Q. Okay. And did you do any analysis to determine whether Grailer could have exfiltrated files from the laptop to a thumb drive without the Digital Guardian reporting it, just by not being connected to the Internet?

MR. YOSHIMURA: Objection.

BY THE WITNESS:

A. Did you ask me if I tested that? I didn't understand the question.

Q. Let me first ask a preliminary question.

Are you saying that you believe Grailer exfiltrated files from her laptop to a thumb drive when she was not connected to the Internet?

Page 35

A. What I'm saying is I found -- and any independent forensic specialist analyzing the same laptop will find the same information that I reference in my declaration that Grailer exfiltrated a significant number of files to an external USB drive.

Q. That's not my question.

My question is: Are you saying that Grailer exfiltrated files from her laptop to her thumb drive when she was -- when the laptop was not connected to the Internet?

MR. YOSHIMURA: Objection.

BY THE WITNESS:

A. What I'm saying is that the Digital Guardian report that I was provided with cuts off at a specific time. I don't have it in front of me. I analyzed that report, obviously, to see if there was any evidence of exfiltration to USB drive. I did not find any in the Digital Guardian report, otherwise, I would have reported that in my declaration.

I did find evidence of exfiltration that any other independent qualified forensic expert can find as well and confirm by analyzing

Page 36

the laptop just as I did.

Q. But it still -- it still just isn't really answering my question. I'm going to try again. It's really at this point just a yes-or-no question.

Are you or are you not -- are you or are you not saying that Grailer was not connected to the Internet when you say that she exfiltrated files from her laptop to her thumb drive?

MR. YOSHIMURA: Objection.

BY THE WITNESS:

A. I don't recall.

Q. I'm just asking if you are saying that.

MR. YOSHIMURA: Objection.

BY THE WITNESS:

A. I don't recall. I'd have to have the Axiom -- Magnet Axiom forensic database in front of me to answer that specific question. I know that Axiom database was provided to your side so that you actually have the ability to answer that question yourself.

Q. Sitting here today, do you know whether or not Grailer's laptop was connected to the Internet during the time that you are claiming she

Page 37

exfiltrated files to her thumb drive?

A. I don't recall.

Q. But I'm just asking do you know.

A. Do I know? I don't recall -- I don't recall performing that analysis specifically. I do recall performing the analysis that's detailed in my report.

Q. I get that.

But you don't remember doing any analysis to determine whether or not Grailer's laptop was connected to the Internet during the time that you say she was exfiltrating files to her thumb drive?

MR. YOSHIMURA: Objection.

BY THE WITNESS:

A. I don't recall.

Q. Okay. But tell me, what is your explanation for the fact that the Digital Guardian report does not record any of the exfiltration that you're alleging she engaged in?

MR. YOSHIMURA: Objection. Asked and answered.

BY THE WITNESS:

A. Well, it sounds like you're asking me

Page 38

to speculate. But I will state, the Digital Guardian report that I was provided with cuts off at a specific time on January 8th. The information that -- the evidence of activities of exfiltration chronologically is after that last time entry in the Digital Guardian report.

So you're asking me to speculate why that information was not transferred from the agent running on the laptop to the Digital Guardian mother ship. I don't know.

Q. Okay. You didn't perform any analysis to try to determine how the Digital Guardian report could have failed to record the copying that you allege, right?

MR. YOSHIMURA: Objection.

BY THE WITNESS:

A. Well, it is not my opinion that the Digital Guardian system failed.

Q. Okay. Well, I'll rephrase the question.

You didn't perform any analysis to try to determine why the Digital Guardian report did not record any of the copying that you allege, correct?

Page 39

A. That's correct. Because I didn't need to.

Q. Okay. And so you can't explain why the Digital Guardian report does not record any of the copying that you allege; is that correct?

MR. YOSHIMURA: Objection.

BY THE WITNESS:

A. I don't recall. I may have performed that analysis. I don't recall. I'll also state it is irrelevant, in my opinion, because the evidence of the exfiltration is on the laptop and can be verified by any qualified peer.

Q. I know you want to talk about that.

But, again, my question is: You can't explain why the Digital Guardian report does not record any of the exfiltration that you allege; is that right?

MR. YOSHIMURA: Objection; asked and answered.

BY THE WITNESS:

A. No. I could explain it if I performed the forensic analysis. In my opinion, I didn't need to because I found evidence of exfiltration on the laptop.

Page 40

Q. You didn't perform the analysis so you can't explain it now; is that correct?

MR. YOSHIMURA: Objection.

BY THE WITNESS:

A. As we sit here, without the benefit of the Axiom database of the laptop, yes. If I had it in front of me and up and running, I could answer your question specifically.

Q. Do you know whether there would be Digital Guardian agent information on Grailer's laptop that was not reported to the Digital Guardian server that you could have reviewed?

A. There could be, but I don't recall looking for that.

Q. All right. I'm going to share my screen here and bring up --

A. Which one am I looking at?

Q. It will be the one that is currently dark. Before we tinker at all with this, Exhibit 4 is displayed on the screen.

Do you recognize Exhibit 4 as a copy of the Digital Guardian report you received?

A. I believe so.

Q. I'm going to stop sharing the screen

Page 41

for a moment. We're moving away from Exhibit 4.

MR. YOSHIMURA: Just for identification purposes, that's obviously a very large document. Larry has only seen a very small sample of it. Is he going to be able to read that document to confirm that what he believes to be the Digital Guardian report is, in fact, the complete report?

MR. SPLITEK: Yes. And I can -- do you want me to send you a copy of it too?

MR. YOSHIMURA: Sure.

MR. SPLITEK: I'll send it to you at our next break. Obviously, you'll get a copy of the digital exhibit in any event.

All right. I'm handing you Exhibit 5.

(Deposition Exhibit No. 5 was introduced to the witness.)

BY THE WITNESS:

A. Okay.

Q. I will tell you that Exhibit 5 depicts information about two entries in the Digital Guardian report marked as Exhibit 4.

A. Okay.

Page 42

Q. Do you have any recollection of seeing the information here in Exhibit 5 before?

A. I don't recall seeing -- seeing these specific entries.

Q. Okay. If you turn to page 2 of Exhibit 5 --

A. Yes.

Q. -- do you see the columns "Destination Device Product Name" and "Destination Device Serial Number"?

A. I do.

Q. Do you recognize that serial number as telling you that this is Grailer's USB thumb drive, the same thumb drive you refer to in your report?

A. It could be. I'd have to cross reference the serial numbers. I don't have it memorized.

Q. Yeah. If you go to paragraph 17 of Exhibit 2, you can do that cross reference.

A. Yes.

Q. So in column FJ on page 2 of Exhibit 5, the destination device serial number, we are seeing the same serial number for the USB thumb

Page 43

drive that you mention in your report.

A. Is that a question?

Q. Right?

A. Yes.

Q. And the two events recorded in Exhibit 5, the timestamp is December 20th, 2022, right?

A. Yes.

Q. And there's, in column CC, it's a destination file path?

A. I do see that.

MR. YOSHIMURA: Matt, I'm going to have to raise an objection here. Because we don't have the actual Digital Guardian report up and we're just working off this printout, I pulled up the Digital Guardian report you have referenced. The columns and rows don't seem to match.

So I think it would be helpful if you would allow the witness to confirm what's in the report rather than confirm what you've put on a piece of paper for him to read.

MR. SPLITEK: All right. I think that will slow things down but if that is what you guys would like to do. I'll share the screen

Page 44

again.

BY MR. SPLITEK:

Q. All right. Mr. Lieb, at your attorney's request we are going to go into the file.

A. Okay.

Q. I'm going to click "enable editing" here on Exhibit 4.

A. Okay.

Q. And then I'm going to go to "data" and I'm going to unfilter and now I'm going to go to column FJ --

A. Okay.

Q. -- for destination device serial number. Are you with me so far?

A. I am.

Q. I'm going to go back to "data" and I'm going to allow filtering.

A. Okay.

Q. So when we -- and you understand you can filter each of these columns to bring up the events that show up, the fields, the values that show up in that column?

A. I do.

Page 45

Q. Okay. So I'm going to only select the number alphanumeric code beginning 070B4.

A. Yes.

Q. And we confirmed that's the serial number for Grailer's USB thumb drive?

A. Yes.

Q. I'm going to hit okay.

And in Exhibit 5, so there were many, many columns, of course, and if we -- you know, we can scroll through here. There is a lot more columns than we want to put on a piece of paper.

But if we -- so Exhibit 5 takes some of those columns, but if we scroll through in column A, the Digital Guardian report in Exhibit 4 matches what's in column A of Exhibit 5, right?

A. Yes.

MR. YOSHIMURA: I'm sorry. I didn't need to make a record of this, Matt.

But the rows that you are showing on the screen right now do not match the row numbers on the piece of paper that you provided. And I cannot confirm that the event time codes, for example, are the same. They don't appear to be contiguous.

Page 46

THE WITNESS: That's odd.

MR. SPLITEK: Okay. In column U, the event codes, what is -- Mr. Yoshimura, what is not matching about the event codes?

MR. YOSHIMURA: So what I see is rows number 5330 and 5331.

MR. SPLITEK: I understand the problem. Here's what your confusion is, I think. Let's unfilter it again and then we will filter and we will go to column U, "event time."

I'm going to sort it oldest to newest and so now the rows will change and I think that is what was confusing, Mr. Yoshimura.

MR. YOSHIMURA: Certainly. Just to make the record clear, Matt, I think what you're explaining to me now is that the paper copy that you provided us is after you resorted all of the data chronologically by which field?

MR. SPLITEK: By -- actually, you can see it right in Exhibit 5. Do you see that in column U next to "event time" there is an

Page 47

arrow pointing upwards?

MR. YOSHIMURA: So you've resorted the entire database by column U in chronological order.

MR. SPLITEK: That is correct.

MR. YOSHIMURA: And once sorted that way, rows 5330 and 5331 are the entries you're referring to.

MR. SPLITEK: Let's confirm to make sure because then we'll sort it. And you can also see this in Exhibit 5, in column FJ there is also another marker there that indicates it is filtered for the field that's appeared in column FJ.

All right. And then let's, in column FJ, do that again. We will select for the serial number and now --

MR. YOSHIMURA: 5330.

MR. SPLITEK: -- 5330, 5331.

MR. YOSHIMURA: Thank you for helping us clarify the record on the reasons for the discrepancies between the database and the paper copy.

MR. SPLITEK: You're welcome. And I

Page 48

will say for the record, the rows on the side are Excel. I don't think that the rows are part of the Digital Guardian report's content. You can reorganize things and the rows will change.

But we see in column A, the user matches, J. Grailer; column U, event time 12/20/22, 6:27 a.m.; column CZ, destination file path, that matches as well.

BY MR. SPLITEK:

Q. And the destination file path, that is to a D drive which is the thumb drive, right?

BY THE WITNESS:

A. Yes.

Q. So that's the file path where the file was copied to?

A. That is my understanding.

Q. Okay. And then the source file path is where the file was copied from; is that correct?

A. Yes.

Q. Okay. All right. And DU, which is detection severity, it is blank in both Exhibit 5 and in Exhibit 4. DZ, event has rule violation. It is blank in Exhibit 5 and Exhibit 4, right? Is

Page 49

that correct?

A. Yes.

Q. Column EH, operation type, file copy is the field in both Exhibit 4 and Exhibit 5, right?

A. You're referring to Exhibit 4?

Q. Well, both of them. Exhibit 4 is on the screen.

A. Oh, sorry.

Q. Exhibit 5 is the paper.

A. Can you repeat the question, please?

Q. Yeah.

It says "file copy" in the operation type column of both Exhibits --

A. I see that.

Q. -- 4 and 5?

A. Yes.

Q. If we go to column ET, was rule violated. The field says no in both Exhibit 5 and Exhibit 4, correct?

A. Correct.

Q. Column FF is destination device. Drive type removable in both Exhibit 4 and Exhibit 5; is that correct?

A. Yes.

Page 50

Q. And that -- actually FI, destination device. Product name is USB disc 2.0 in both Exhibit 4 and Exhibit 5, correct?

A. Correct.

Q. And column FJ, in both exhibits it is the serial number?

A. Correct.

Q. So if we go back to column FF, the destination drive, it is telling you that's something that Grailer can remove from the computer?

A. Yes.

Q. And then if we go to source device drive type in column GG -- I apologize -- column GD, source device drive type is fixed. The source device is where-- that's the drive where it is coming from, correct?

A. Yes.

Q. And then column GE -- column GG, source device product name in both Exhibit 4 and Exhibit 5 it's a Samsung. Is that the hard drive for Grailer's laptop?

A. I believe so.

Q. And then you also see in Exhibit 4 and

Page 51

5 column GH match, right?

A. They do.

Q. Okay. And then column IR, source was classified. That matches as well, right?

A. Column IR has the value "no" in both rows for sources classified.

Q. Yep. In both Exhibit 4 and Exhibit 5, right?

A. Yes.

Q. Okay. So when I -- I won't want to do this for every exhibit here, but we've been able to go through Exhibit 4 and Exhibit 5 to understand how the Exhibit 5 information was extracted from Exhibit 4, right?

MR. YOSHIMURA: Yes. And just for the record, to the extent a similar exercise may be needed in the future, we're agreeable to not go through this every time, but we need to make a record clear of how the paper copy is derived from the data in the database.

MR. SPLITEK: Understood. And also having been through this exercise, even after the deposition too, you feel like, Mr. Lieb, you'd be able to verify using the Excel

Page 52

spreadsheet whether anything in any of these paper exhibits is going to be incorrect, right.

THE WITNESS: I would be able to, yes.

BY MR. SPLITEK:

Q. Okay. As long as we have Exhibit 4 up, I'm going to stay in Exhibit 4, I'm going to unfilter again.

A. Okay.

Q. I'm going to go back to event time.

A. Okay.

Q. I'm going to filter, or I'm going to try to. Yes, now I've done it.

And now I'm going to sort newest to oldest in event time.

A. Okay.

Q. And do you agree that should bring up at the top the latest event in the Digital Guardian report, right?

A. Yes.

Q. Let's try again. We're going to sort newest to oldest. So the latest event that we're seeing in the Digital Guardian report is 9:28 p.m. on January 8th, 2023; is that correct?

Page 53

A. That is correct.

Q. Okay.

MR. SPLITEK: I'm going to pull down Exhibit 4 now. I'm going to hand you Exhibits 6 and 7.

THE WITNESS: Okay.

(Deposition Exhibit Nos. 6 and 7 were introduced to the witness.)

BY MR. SPLITEK:

Q. If you look at -- if you look at both Exhibit 6 and Exhibit 7, do you see, again, that up-facing arrow next to the event column, event time in column U?

A. I do.

Q. Okay. So I'm telling you that that is because I sorted before making these paper exhibits the information in chronological order, not reverse chronological, but chronological.

And in Exhibit 6 and 7, if you see the top row in Exhibit 6 is a January 7th, 2023, entry, right?

A. I do see that.

Q. Okay. And if you look at the bottom

Page 54

row in Exhibit 7, the last row --
A. Bottom row in Exhibit 7.
Q. -- is the same time that we just saw, am I right? 9:28 p.m. on January 8th, 2023?
A. On Exhibit 7 are you referring to Excel row 8345?
Q. That's correct?
A. Okay.
Q. Do you see there's that same 9:28 p.m. timestamp on January 8th, 2023?
A. On Exhibit 7, Excel row 8345, column U it says January 8th, 2023, 9:28.
Q. Okay. And I don't want to go through recreating this again live on the screen, but I'm telling you that Exhibit 7 -- back up.
I'm telling you that Exhibit 6 shows some of the columns on all of the events that the Digital Guardian reported on the first part of January 8th, 2023.
Do you understand?
A. Say that again.
Q. Exhibit 6.
A. 6.
Q. I'm telling you that this is showing

Page 55

data on all of the events that Digital Guardian recorded --
A. Okay.
Q. -- during the first part of January 8th, 2023.
Do you understand?
A. I do.
Q. And then in Exhibit 7, what's depicted is all of the rest of the events that Digital Guardian reported on January 8th, 2023 in chronologic order.
Do you understand?
A. I do. Although -- I don't have access to all of the rows and columns. I just have the ones that are visible in your exhibits.
Q. Well, you have access to all of the rows but not -- I see what you mean. You don't have access to all of the rows of the Digital Guardian report?
A. Correct.
Q. Yeah, that's right. Exhibits 6 and 7 show only some of the rows and only some of the columns.
A. Yes.

Page 56

Q. Because as we just saw in Exhibit 4, it is quite unwieldy, isn't it?
A. Well, I see, for example, on Exhibit 7 it is column EH, the second row down, it says "file copy" but I don't see any other columns about what was -- where that was copied to.
Q. I'm sorry. What are we looking at right now?
A. Exhibit 7, second page, the second row down which is -- I didn't bring my glasses, unfortunately, 8303. It's a file copy, Illinois River Energy.MSG, which is an e-mail file. It says "file copy." But I don't see any other copies about where the destination was.
Q. Yes. That's correct. The -- well, actually maybe not. If you look -- so you're looking at row 8303, is that correct, on Exhibit 7?
A. I am.
Q. Okay. What about if you turn back to page 1, the destination file path?
A. Okay. So this is -- so page 1 is other additional columns of the same rows.
Q. That's correct. Yes, to also clarify,

Page 57

if you look at the rows on page 1 and 2 of Exhibit 7, the rows match, and that's because there are so many columns in Exhibit 4 that for -- you were looking at row 8303, right?
A. Yes.
Q. So page 1 gives you some columns for row 8303, and when you flip to page 2 there are more columns for the same row 8303?
A. I understand.
Q. So, for example, then, in row 8303, you pointed out in column EH, the operation type is a file copy, right?
A. Yes.
Q. And in page 1 in the destination file path column, the Digital Guardian report tells you that the file was copied to what appears to be Grailer's INetCache folder; is that correct?
A. Yes, it does.
Q. And what is the INetCache folder?
A. That is -- my understanding is a Windows Explorer/Internet browser system file that records human activity.
Q. That's what the INetCache folder shown in the destination file path column is?

Page 58

A. That's my understanding of what INetCache is, yes.

Q. Okay. Do you know whether or not the INetCache folder contains copies of temporary files?

A. I don't know if I characterize it as a temporary file. I would characterize it as a system file.

Q. Do you know when somebody adds an attachment to an e-mail, do you know if it is saved to an INetCache folder like we're seeing here in row 8303 of Exhibit 7?

A. I don't know.

Q. Do you know whether when someone opens an attachment to an e-mail it is saved to an INetCache folder like we're seeing here in 8303 of Exhibit 7?

A. I don't know.

Q. Do you know whether after a file is, for whatever reason, saved to the INetCache folder, it is then automatically deleted later?

A. Your question is whether that file is saved to that folder? That's -- your question doesn't actually make sense. So the INetCache is

Page 59

a system file that's recording -- my understanding it's recording activity. So it's not holding a copy of a file, per se. It's recording activity a user of a laptop is performing using Windows Explorer and an Internet browser.

You asked me specifically if it is keeping a copy of the file, so I wanted to be clear that's --

Q. And let me point out in column CZ, destination file path in row 8303 of Exhibit 7, do you see after INetCache it says "content.outlook"?

Do you see that?

A. Which row?

Q. Exhibit 7, row 8303, column CZ, destination file path.

A. Okay.

Q. Do you see the INetCache and then content.outlook after that?

A. I do see that, yes.

Q. Okay. So do you think that this has something to do with e-mail activity or web browsing?

A. I don't know. I'd have to analyze that specific file on the laptop to answer that

Page 60

question.

Q. All right. Am I right, though, that you're not sure how the INetCache folder works?

A. I've analyzed laptops and have encountered the INetCache folder many times. So my understanding is that it's a system -- it's a system artifact that is generated when a user is performing activities on a laptop.

Q. And it is not a folder then that the user is adding copies of files to and deleting copies of files to on purpose typically, right?

A. That's the distinction I'm making. It is the result of a system. So it's not a file that a user would go "I'm going to open this up and interact or copy files to this location."

Q. Okay. Got it. So activity in Grailer's INetCache folder, you would expect that typically the user like Grailer wouldn't be aware of what's happening in the INetCache folder?

MR. YOSHIMURA: Objection.

BY THE WITNESS:

A. I don't believe most computer users are aware of how Window's system files work.

Q. Okay. So Exhibits 6 and 7, they

Page 61

provide information about, taken together, all of the events that Digital Guardian recorded on January 8th, 2023. I'm telling you and you're able to verify that later by looking at Exhibit 4, right?

A. If you're asking me if these Exhibits 6 and 7 represent information that was captured and recorded by Digital Guardian, then, yes, that is my opinion.

Q. And you can figure out later if I've accidentally left something out from this record of the January 8th, 2023 events, right?

A. I could. And I don't have any evidence that you've left anything out.

Q. When you were reviewing the Digital Guardian report, did you review its records about events on January 8th, 2023?

A. I did.

Q. Okay. And you did not find any evidence of exfiltration on January 8th, 2023 in the Digital Guardian report, correct?

A. Correct.

Q. But back in Exhibit 5, which we painstakingly verified using Exhibit 4 on the

Page 62

screen, we did see a record in Digital Guardian of Grailer copying files to the same USB thumb drive that you referenced in your report, right?

A. I do see in the Exhibit 5 evidence captured in the Digital Guardian report of Jessica Grailer copying a file, drug screen registration instructions.PDF and epassport_wd-121822-5u2yd.pdf from a folder on her C drive to -- what I refer to as the Emtec USB drive on December 20th, 2022.

Q. And so in Exhibit 5 Digital Guardian recorded the date and time of the copying, right?

A. It did.

Q. And it recorded the name of each file that Grailer copied, right?

A. It did.

Q. And it recorded the drive and folder that the file was copied from; is that right?

A. It did.

Q. And it also recorded the drive and folder that the file was copied to, right?

A. Correct.

Q. And it recorded the serial number of the USB thumb drive that it was copied to?

A. It did.

Page 63

Q. And, to your knowledge, does the Digital Guardian report record Grailer copying any files to that USB thumb drive again after December 20th, 2022?

A. I did not find any evidence within the Digital Guardian report of any file copying activities on January 8th.

Q. Did you look at the period from December 21st through January 7th, 2023?

A. I analyzed the entire report as part of my forensic analysis process.

Q. Do you know of any other instances other than the two shown in Exhibit 5 where Digital Guardian recorded Grailer copying files to the USB thumb drive that you discuss in your report?

A. I don't recall.

Q. And don't you want to know why, if Digital Guardian recorded all of the information shown in Exhibit 5, it didn't record similar information on January 8th, 2023?

MR. YOSHIMURA: Objection; asked and answered.

Page 64

BY THE WITNESS:

A. I stand by the findings in my declaration, and any independent qualified forensic expert analyzing Jessica Grailer's laptop will come to the same conclusions as the evidence is independently verifiable.

Q. But that wasn't quite my question.

My question is: We know that -- we saw it in Exhibit 5, Digital Guardian recorded quite a bit of information about instances where Grailer copied files to her USB thumb drive on December 20th, 2022, right?

A. In the exhibit there is two examples.

Q. That's right. And it recorded quite a bit of information about those two examples, correct?

A. Recorded the source destination, the make, model, serial number of the USB drive used, which is the Emtec drive, as I refer to in my report, and recorded the date and time of the file copying.

Q. So my question earlier and I'll ask again was: Don't you want to know why the Digital Guardian report did not record any such information about any copying events on January 8th, 2023?

Page 65

MR. YOSHIMURA: Objection; asked and answered multiple times at this point.

BY THE WITNESS:

A. So my declaration contains wholly 100 percent scientific and independently verifiable evidence of Grailer exfiltrating files and all of the information that I cite in my declaration refers to specific evidence located on her laptop, the forensic image of her laptop, and can be independently verified by any qualified peer.

Q. I know you're attorney has said that it is asked and answered. I don't think it was answered.

But I'm going to assume that you don't want to know why Digital Guardian did not report the kind of information that we see in Exhibit 5 for any events on January 8th, 2023. If I'm wrong, tell me.

MR. YOSHIMURA: Objection.

BY THE WITNESS:

A. In my opinion, your question doesn't make sense. It's irrelevant. The evidence that I

Page 66

found of Grailer's acts are independently verifiable by any qualified peer analyzing her laptop.

Q. So in Exhibit 7 --

A. Okay.

Q. -- we can see that the last entry in the Digital Guardian report is at 9:28 p.m. on January 8th, 2023, right?

A. I see that.

Q. Okay.

A. Wait. Which row?

Q. It is the last row at the bottom of -- well, the row is at the bottom of both pages of Exhibit 7, but the event time is in column U on page 1 of Exhibit 7.

A. Okay.

Q. And in row 8345 we see that the last event recorded in the Digital Guardian report is 9:28 p.m. on January 8th, 2023, correct?

A. That is correct.

Q. And we also verified that by looking at the Digital Guardian report in its original Excel form, Exhibit 4, right?

A. We did.

Page 67

Q. All right. So are you saying that all of the exfiltration that you allege occurred after 9:28 p.m. on January 8th, 2023?

A. I'm saying that the evidence that I reference in my expert report, which I'd -- you'd have to get more specific about times and dates, are independently verifiable by any qualified peer.

Q. Except it just doesn't answer my question because I'm -- this is just yes or no.

So 9:28 p.m. on January 8th, 2023, there were times before 9:28 p.m. on January 8th, 2023, right?

MR. YOSHIMURA: Objection.

BY THE WITNESS:

A. So I did not find any evidence of exfiltration within the Digital Guardian report, which is why I didn't reference it in my expert report.

Q. I'm not asking you that. I'm asking you: Are you claiming that Grailer exfiltrated files before 9:28 p.m. on January 8th, 2023?

A. In my expert report, I detail evidence of exfiltration, consistent with exfiltration bulk

Page 68

filing -- file copying, and it's independently verifiable by any qualified peer.

Q. I'm going to ask the question again. Yes or no, are you claiming that Jessica Grailer exfiltrated any files at any time prior to 9:28 p.m. on January 8th, 2023?

A. I don't recall. You'd have to look -- I'd have to look at my report and what's detailed in my report. Can you ask me something specific in my report?

Q. So is the answer that you don't know?

A. I don't have my report memorized, as I sit here. I can -- if you ask me a specific question about the information I have in my declaration, I'll answer that question.

Q. Okay. So you might be claiming that Jessica Grailer exfiltrated files before the last entry in the Digital Guardian report, correct?

MR. YOSHIMURA: Objection.

BY THE WITNESS:

A. What I'm saying is that all of the evidence that I reference in my report has footnotes to exactly where that evidence exists on the forensic image of Jessica Grailer's laptop and

Page 69

all of that evidence can be independently verified and replicated by a qualified peer.

Q. I'm going to do this one more time. And I'm just going to tell you, I think it is very likely I'll move to compel an answer after the deposition.

Yes, no, or you don't know. Are you or are you not claiming that Jessica Grailer exfiltrated any files before 9:28 p.m. on January 8th, 2023?

A. I got to review my declaration to answer that question.

Q. Go ahead. Can you, for the record, say what exhibit are you looking at? What is the exhibit number?

A. I'm looking at Exhibit 2. I'm referring to paragraph 17. It says [as read]: Forensic analysis of Ecolab laptop revealed Jessica Grailer last connected an Emtec serial number USB drive to her Ecolab laptop on January 8th, 2023 at 9:39 p.m., which is 10 minutes after the Digital Guardian report ends.

Q. So are you --

A. And that's why I stated earlier that

Page 70

the evidence of exfiltration that I describe in the report, you asked me multiple times why do I not see this in the Digital Guardian report, I've answered multiple times. I found no evidence of exfiltration in the Digital Guardian report. If I did, I would report it. I'm an independent expert.

It clearly states in my declaration here on 17 that she connected the drive that, in my opinion, she used to exfiltrate the Emtec drive, the same drive that was connected to her laptop as recorded by the Digital Guardian report on 12/20/2022, was done at 9:39 p.m.

I have a footnote so that any independent expert can look at that same laptop, that same forensic artifact, and confirm exactly what I'm saying. I'm not making up that time and date. That is exactly what is recorded by the laptop.

Q. So am I right then in inferring that you are saying that all of the exfiltration that you allege occurred after 9:39 p.m. and 51 seconds on January 8th, 2023?

MR. YOSHIMURA: Objection.

Page 71

BY THE WITNESS:

A. I'll read my declaration. So it says [as read]: Forensic analysis of the Ecolab laptop revealed Jessica Grailer last connected an Emtec 32 gigabyte drive, serial number 070B4A71ADB22353, what I'm referring to as the Emtec drive, to her Ecolab laptop on January 8th, 2023, at 9:39 p.m.

My next paragraph says [as read]: Forensic analysis of her Ecolab laptop revealed Jessica Grailer accessed and exfiltrated multiple files on January 8th, 2023 including the 259 files described in Exhibit E based on -- what should be my forensic analysis. It is my opinion that the 259 exfiltrated files were copied by Jessica Grailer to the Emtec drive on January 8th, 2023.

That is my opinion that can be independently verified by any qualified peer.

Q. Okay. But in paragraph 18 you did not write the time that you said the exfiltration occurred.

So my question -- I'm going to ask this again. The exfiltration that you allege in paragraph 18, are you claiming that that occurred all after the connection event that you allege --

Page 72

A. Yes.

Q. -- in paragraph 17?

A. Yes.

Q. Okay. So the exfiltration that you claim Grailer engaged in, in your view, all occurred after 9:39:51 p.m. on January 8th, 2023, correct?

A. Correct. That's my opinion why it's not appearing in the Digital Guardian report.

Q. Got it. So you are not opining that Jessica Grailer exfiltrated any files at any time before 9:39:51 p.m. on January 8th, 2023; is that correct?

MR. YOSHIMURA: Objection; misstates testimony.

BY THE WITNESS:

A. I believe you're mischaracterizing what I'm stating in my expert report.

So a couple items. One, you asked earlier isn't it true that the Digital Guardian report shows on December 20th, a connection of this Emtec drive. I said it absolutely does.

Then the forensic analysis of her laptop shows that she last connected, according to

Page 73

my two forensic tools, the same Emtec drive to her laptop on 9:39 p.m. which is after the last time entry in the Digital Guardian report.

Q. I understand all of that. I thought that what I was asking you to agree with just flowed from what you already said. So let's back up and do this again.

You are opining in this case that Jessica Grailer exfiltrated files on January 8th, 2023, right?

A. That is my opinion based upon my independent forensic analysis of the evidence existing on her work laptop.

Q. And I thought you just told me this a few moments ago, but are you opining that all of that exfiltration that, in your view, happened all occurred after the 9:39:51 p.m. on January 8th, 2023 time that you identify in paragraph 17 of your report?

A. So it is my opinion based upon -- in paragraph 18, that these 259 files described on Exhibit E3 were exfiltrated by and copied by Jessica Grailer to this Emtec drive on January 8th, 2023.

Page 74

Q. Yep, but that's not my question.
So is it your -- I understand because you wrote it right there in your report that it is your opinion that Jessica Grailer exfiltrated files on January 8th, 2023.
I want you to focus on the time that you wrote in paragraph 17. 9:39:51 p.m. on January 8th, 2023. Just stay focused on that time.
A. So what --
Q. I have not asked the question yet. I want you to focus on that time.
A. Okay.
Q. And I want you to think about the time before that time and the time after that time.
A. Okay.
Q. Make 9:39 p.m. on January 8th, 2023, that's a dividing line here. Are we on the same page so far? Do you understand what I'm just saying? Just focus on 9:39 p.m. on January 8th, 2023.
A. Well, except for the fact that in exhibits -- if we look at Exhibit F -- I believe it is Exhibit F.

Page 75

Q. Okay. Let me make sure the record is clear. Are you in Deposition Exhibit 3, right now?
A. Sorry. Yes, I am in Exhibit 3, to be clear.
Q. Deposition Exhibit 3.
A. Exhibit 3.
Q. Exhibit F to your report.
A. Right.
Q. All right. Actually, let me -- I have it as a freestanding exhibit. Let's make the record a little cleaner.
MR. SPLITEK: I'm going to hand you Exhibit 36 out of order.
(Deposition Exhibit No. 36 was introduced to the witness.)
BY MR. SPLITEK:
Q. So you tell me, is Exhibit 36 a copy of Exhibit F to your report?
A. Yes.
Q. Great.
What would you like to tell me about Exhibit F to your report?
A. What I see -- and I came to this

Page 76

exhibit during my process of crafting my response to Mr. Pixley's report. And I noted in my forensic tool that I found evidence of bulk rapid selection of multiple files.
For example, on the -- I'll call it -- I'll call it the first page or the second page or third page, we see that there's a file called ADM2019plan.doc going all the way down to tier two, 2021.xls. It is a master file table date of 8:33 p.m. and they're all within microseconds of each other.
From my experience and analysis in many, many cases, this is -- sort of evidence is consistent with an individual bulk selecting, zipping, copying data. This evidence is inconsistent with a human being rapidly opening up each individual files, you know, within microseconds. That just doesn't make any sense.
Q. Okay.
A. Sorry. Go ahead.
Q. So let's just focus on the first page of Exhibit F so we're looking at something concrete here.
A. Okay.

Page 77

Q. There's a bunch of timestamps there for 12:41:32 on January 8th, 2023, right?
A. Yes.
Q. And by the way, what offset did you use when converting that from UTC to Central Standard Time?
A. I believe that is Central Standard Time in my database. But I believe I set it at Central Standard Time in OSForensics.
Q. Is it possible that you --
A. It's UTC?
Q. Well, no.
Is it possible that you prepared it after we went back to Daylight Savings Time and used the wrong offset?
A. I don't have any recollection of doing that.
Q. Anyway, we see timestamps that are all much earlier on January 8th, 2023 than 9:30 p.m., right?
A. We do. And it is also important to note these are actually folders. These are not files.
So I would have to address each of the

Page 78

files listed in there, I'd have to expand that out. I can if I'm asked to do that.

Q. So if we turn to the next page.

A. Okay.

Q. So this is page 2 of your Exhibit F?

A. I see that.

Q. So there's files listed there, right?

A. I do see them.

Q. And there's identical timestamps of 8:33 p.m.?

A. Yes.

Q. And that's still earlier than the last entry in the Digital Guardian report, right?

A. It is.

Q. Okay.

A. And I have not analyzed this, but it would be interesting to search in the -- because this is clearly evidence of bulk selecting and interacting with these files, in my opinion, not individually opening them up one at a time.

It is possible someone could have mistakenly selected all of these files and hit open. I found no evidence of that.

But it would be interesting to look at

Page 79

the Digital Guardian report to see if the access of these files, so, for example, the ADM2019.plan.docx on page 2, which was at 8:33 p.m. is in the Digital Guardian report. I didn't look -- I didn't search for that file in the Digital Guardian report during my analysis.

Q. So are you claiming that Grailer exfiltrated files to her USB thumb drive around 8:33 p.m. on January 8th, 2023?

A. What I'm stating is exactly what I say in my report, is that this evidence is consistent with an individual I believe to be Jessica Grailer bulk selecting huge numbers of files to copy them, zip them.

Q. This is just a yes-or-no question.

I want you to look at page 2 of your Exhibit F.

A. Okay.

Q. There are a bunch of files there with timestamps of 8:33 p.m. on January 8th, 2023.

A. Yes.

Q. Are you or are you not claiming that Jessica Grailer exfiltrated those files around 8:33 p.m. on January 8th, 2023?

Page 80

A. I'm claiming that she -- and the forensic evidence is consistent with the fact that she, an individual I believe to be Jessica Grailer, bulk selected and interacted with these files. And this is consistent with evidence of dragging and dropping them to an external media, zipping them, exfiltration.

So it's consistent with exfiltration, yes.

Q. And I'm going to ask it again. It is a yes-or-no question. I'm only going to ask it once more. I'm going to tell David again. If I'm not getting an answer, I'm probably going to move to compel.

If you look at, just for -- you know, there is a lot of timestamps in your Exhibit F.

A. Okay.

Q. We're looking for an example of -- on page 2 of your Exhibit F, the files that have an MFT modified date timestamp of 8:33 p.m.

A. I see that.

Q. So yes, no, or you don't know, are you or are you not claiming that Jessica Grailer did exfiltrate those files at that time of 8:33 p.m.

Page 81

on January 8th, 2023?

MR. YOSHIMURA: Objection; asked and answered.

BY THE WITNESS:

A. Yeah, this evidence of rapid interaction with multiple files, from my experience, is consistent with an individual exfiltrating files, bulk selecting, copying files, yes. I've never seen evidence -- I have no evidence in this case that this is evidence of someone rapidly within microseconds opening up files one at a time.

So in my opinion, this evidence is consistent with an individual I believe to be Jessica Grailer exfiltrating these files.

Q. At 8:33 p.m. on January 8th, 2023?

A. Yes.

Q. How could Grailer exfiltrate the files shown on page 2 of your Exhibit F at 8:33 p.m. on January 8th, 2023, without Digital Guardian recording that copying?

A. I don't know. As I stated earlier, I found no evidence of exfiltration by Grailer within the Digital Guardian report because,

Page 82

otherwise, I would have reported on that.

But I found significant evidence of -- independently verifiable evidence of Grailer exfiltrating files from her laptop on the laptop itself.

Q. But now we've established that it is your opinion that Grailer exfiltrated files to her USB thumb drive before the last entry in the Digital Guardian report, right?

A. It is my opinion that this evidence is consistent with an individual I believe to be Jessica Grailer bulk selecting files and folders on January 8th, which is consistent with my experience with exfiltration.

Q. And doing that before the last entry in the Digital Guardian report, right?

A. In my opinion, on page 2 of Exhibit 36, I see a bunch of loose files that were all selected at 8:33:25 microseconds, some of them are 24, or milliseconds -- or seconds, sorry, that's seconds, 25 seconds.

So, yes, that evidence is consistent, in my opinion, with an individual I believe to be Jessica Grailer selecting those files and exfiltrating them, yes.

Page 83

Q. And so your opinion is that Jessica Grailer exfiltrated files to her USB thumb drive during a time when the Digital Guardian report was still recording entries but without her exfiltration being recorded in the Digital Guardian report?

A. Now, you're mischaracterizing what I'm saying. So I don't have the Digital Guardian report in front of me.

Again, what I would recommend is you can have me do it, you can do it, is search for these file names within the report. Because this evidence is obviously independent. It is clear that an individual I believe to be Jessica Grailer bulk selected these files, interacted with these files all on January 8th at 8:33 p.m.

So is that -- I don't know if those -- I did not look to see if those files were in the -- evidence of that interaction were in the Digital Guardian report, but it would be interesting to see.

Q. If Grailer exfiltrated files to her USB thumb drive at 8:33 p.m. on January 8th, 2023, would that exfiltration be recorded in the Digital Guardian report?

Page 84

A. What I'll state is that I don't -- I found no evidence of exfiltration within the Digital Guardian report. I did find evidence that can be independently verified by any qualified peer of significant file exfiltration as detailed in my expert report.

Q. That wasn't my question.

My question is: If Grailer exfiltrated files to her USB thumb drive at 8:33 p.m. on January 8th, 2023, would you expect to see that exfiltration recorded in the Digital Guardian report?

A. Again, I'm an independent expert. I do not have -- well, I have not searched the Digital Guardian report for these particular file names that I'm seeing -- that I'm seeing that she bulk interacted with, in my opinion, at 8:33 p.m. on January 8th.

If you have the Excel spreadsheet I think I would recommend doing a search for one to see if one appears in that report and see if Digital Guardian reported this interaction that clearly exists on the laptop.

Page 85

Q. But that wasn't my question.

My question is -- just try to focus on what I'm saying here. If Grailer exfiltrated files to her USB thumb drive at 8:33 p.m. on January 8th, 2023, would you expect to see that exfiltration recorded in the Digital Guardian report?

A. I don't know.

I do know that the evidence here of exfiltration can be independently verified by any qualified peer. I don't know why these ones -- the OSForensics, which, again, I came to through analysis in response to the Pixley declaration.

So, for example, I don't see -- there's multiple files or folders -- I'm referring to Exhibit 36, the first page. I see a huge number of folders that were all bulk selected and interacted with at 12:41 p.m., which is prior to the 9:28 p.m. cutoff of the Digital Guardian report.

But, again, we'd have to look at the individual files within there to see what those access dates were, those interaction dates were.

Page 86

I didn't do that for the purposes of this. I just noted that, as I state in my -- let's see. Forensic analysis of the Ecolab laptop also revealed that Jessica Grailer accessed multiple additional files and folders in rapid succession on January 28th, 2023 [sic]. That is independently verifiable.

I've included six screen shots of the Ecolab which display the files and folders accessed by Jessica Grailer on January 8th, 2023, as Exhibit F. Due to the fact that it is impossible for a human being to access and open hundreds of files within seconds of each other, it is any opinion that Jessica Grailer copied those files and folders to the Emtec drive on January 28th, 2023, in addition to the files described in Exhibit E.

Those files don't appear in the Digital Guardian report, as I've stated multiple times. I don't see any evidence of exfiltration within the Digital Guardian report. I do not have an explanation why.

But I do have and I'm referencing independently verifiable evidence that is

Page 87

consistent, in my experience, with exfiltration on her laptop.

Q. You have no many explanation as to how Grailer could have exfiltrated files to her USB thumb drive before the Digital Guardian reports' last entry without Digital Guardian recording that activity, right?

A. I have no explanation, as I'm sitting here, why Digital Guardian did not report on the activity that is clearly -- clearly exists and is independently verifiable on a laptop as I'm describing in paragraph 19.

Q. You testified in your February 2023 declaration that the Digital Guardian report covered activities through and including January 18th, 2023; is that right?

A. No. The Digital Guardian report only goes up to, and I'm trusting that this is the last line that you're displaying in Exhibit 7, 9:39, activity after her last date of employment was captured and recorded by Office 365's audit log, which I know was produced as a file called JGrailer.Excel. And then later on more data was recovered from a tool called Elastic that Ecolab

Page 88

uses.

MR. SPLITEK: I'm handing you Exhibit 8.

(Deposition Exhibit No. 8 was introduced to the witness.)

BY THE WITNESS:

A. Okay.

Q. This is a copy of your February 2023 declaration, right?

A. Okay.

Q. Is that correct?

A. Exhibit C?

Q. Well, I've marked it as Exhibit 8.

A. Sorry. Yes. Yes. So Exhibit 8, yes, Exhibit 8.

Q. Is your February 2023 declaration?

A. Okay.

Q. Is that right?

A. I'm reviewing it.

Yes. And I see where you say in -- in paragraph 15 it says January 18th, 2023 so that's a typo. It should be January 8th, 2023.

Q. Okay. And let's look at this actually at page 3 in your February 2023 declaration.

Page 89

A. Okay.

Q. You begin a section called "Forensic Analysis, Digital Guardian Report."

A. Okay.

Q. Right? Is that correct?

A. It is.

Q. Okay. And then it looks to me like the next section doesn't begin until paragraph 19; is that correct?

A. That is correct.

Q. Okay. So in paragraph 15 you testified that [as read]: Ecolab's data loss prevention tool, Digital Guardian Version 8.4.0.0263 generated a report of all interactions former employee Jessica Grailer performed regarding Ecolab files during the period November 14th, 2022 through January 18th, 2023, inclusive."

A. Okay.

Q. Is that right?

A. Yes.

Q. And then you said that you forensically analyzed the Digital Guardian report and came to the forensic observations and opinions set forth in your declaration; is that right?

Page 90

A. Yes.

Q. And then the next paragraph you talk about an event on January 14th, 2023, correct?

A. It says paragraph 16, Exhibit 8 [as read]: Forensic analysis revealed Jessica Grailer accessing her Ecolab OneDrive account using a heretofore undisclosed iPhone 12 mini on January 14th, 2023."

The evidence of this appears in a file that was provided to me by Jennifer Semmler of Ecolab IT called JGrailer.xlsx. That file is actually an Office 365 audit log. That audit log -- the Office 365 audit log, my understanding, upon information and belief, I was provided a copy with was also supplemented by a -- with more columns from -- as it was restored from a tool called Elastic that Ecolab uses to aggregate logs in an automated fashion.

Q. But why in your February 2023 declaration did you not mention the document that you had gotten from Jennifer Semmler?

A. I don't recall, but it's possible that the date that I wrote this I assumed that the JGrailer.Excel file, which is actually -- that's

Page 91

the post -- posted last date of employment was also a Digital Guardian tool.

So I should have been -- I could have been more specific. I guess at the time I wrote this I assumed that those two reports were both from Digital Guardian. That is not correct.

The Digital Guardian report only goes through January 8th and then subsequent activity post her January 8th derives from the Office 365 audit log that was originally provided to me as a file named JGrailer.xlsx and then later supplemented by Office 365 audit log data that that was restored from Ecolab's Elastic system.

Q. Understood.

I want you to take a look at -- still in Exhibit 8.

A. Okay.

Q. Let's go to paragraph 24 of your February 2023 declaration.

A. Okay.

Q. No. Check that.

Let's go to paragraph 24. Did I say that right? Paragraph 24 of your February 2023 declaration.

Page 92

A. Okay.

Q. In paragraph 24 of your February 2023 declaration you testify that forensic analysis of the laptop had revealed Jessica Grailer exfiltrating multiple photographs. And you say that happened at 9:11 p.m. on January 8th of 2023, correct?

A. Forensic analysis of the laptop revealed Jessica Grailer exfiltrating multiple photographs of Ecolab equipment from her Ecolab OneDrive account and taken by her iPhone 6S.

It doesn't say like on January 8th, 2023, 9:11 p.m. It doesn't have a verb after that. But I recall that my forensic analysis of photos, it had this iPhone 6S metadata imbedded in the photographs. And that's how I came to the opinion that these photographs were taken by that phone.

Q. Were you or were you not saying in paragraph 24 of your declaration that the alleged exfiltration occurred at 9:11 p.m. on January 8th, 2023?

A. I believe that is what I am saying. I'm just looking at -- it's like a footnote.

Page 93

Let's see.

It says -- which is coming from the decrypted image, OneDrive pictures, Adkins Evap inspection, September 23rd, 19. Evap overview, pictures and IMG3654.jpeg.

So that's the file -- my recollection is a forensic analysis of this picture file, IMG6354.jpeg was -- the embedded metadata shows it was taken by an iPhone 6S.

Q. But that's not my question.

My question is: Were you saying that the exfiltration you were alleging in paragraph 24 occurred at 9:11 p.m. on January 8th, 2023?

A. As I read that, I'd say yes.

Q. Okay.

A. But I'd have to look at the -- I don't have the forensic database.

Q. Let's turn to paragraph 30 of your February 2023 declaration.

A. Okay.

Q. In paragraph 30 of your 2023 declaration you testified that Jessica Grailer exfiltrated files at 7:20 p.m. and 8:48 p.m.?

A. Sorry, which paragraph?

Page 94

Q. Paragraph 30.

A. Okay.

Q. You testified that Jessica Grailer exfiltrated files at 7:20 p.m. and 8:48 p.m. on January 8th, 2023.

A. Okay.

Q. Correct?

A. Yes, that is what my declaration states.

Q. Okay. And you would agree that both of those times are earlier than the last entry in the Digital Guardian report?

A. Yes.

Q. All right.

A. I'd also like to state that in paragraph 29 I'm seeing that forensic analysis of the laptop revealed Jessica Grailer accessing the below folders and files from the Emtec USB drive. It shows the same D, June 22nd VR meeting, VR Nalco, evaporative inspection with performance index PDF.

And so as I sit here, I don't recall searching for these file names through the Digital Guardian report, but I probably did. But you

Page 95

could actually search for them now because it clearly -- again, this is independently verifiable through a forensic analysis of her laptop that Jessica Grailer had these folders on her Emtec drive containing these files.

Q. I want you to turn to paragraph 31 of your February 2023 declaration.

A. Paragraph which?

Q. 31.

A. Okay.

Q. In paragraph 31 you testified that Jessica Grailer exfiltrated a document at 8:56 p.m. on January 8th, 2023, right?

A. Yes.

Q. And, again, that's before the last entry in the Digital Guardian report, correct?

A. Yes.

Q. All right. Look at paragraph 32.

A. Okay.

Q. You testified that Grailer exfiltrated files at 7:33 p.m. and 9:04 p.m. on January 8th, 2023, correct?

A. Yes.

Q. And that, again, was before the last

Page 96

entry in the Digital Guardian report, right?

A. Yes.

Q. Okay. Paragraph 33 you testified that Grailer exfiltrated files at 9:11 p.m. on January 8th, 2023, right?

A. Yes.

Q. And, again, that was before the last entry in the Digital Guardian report?

A. Yes.

Q. Okay. Why did you never mention in your report in Exhibit 2 that the Digital Guardian report does not show Grailer copying any files to her thumb drive on January 8th, 2023?

A. Well, I found no evidence of exfiltration of files through my analysis of the Digital Guardian report so I didn't refer to any analysis because I didn't find any evidence of exfiltration as recorded by the Digital Guardian report.

My evidence of exfiltration all derived from -- and can be scientifically and independently verified through analysis of her work laptop.

Q. So you only put in your report

Page 97

information that you thought supported the conclusion of exfiltration; is that right?

MR. YOSHIMURA: Objection; leading, argumentative.

BY THE WITNESS:

A. My reports all contain evidence -- you'll notice they're all footnoted.

Q. That is not my question. I'll ask it again and you can answer it or not.

But in your report, you agree you've never disclosed that the Digital Guardian report does not record any of the exfiltration that you allege, right?

A. The question doesn't make sense because I did not find evidence of exfiltration recorded by the Digital Guardian report. I found evidence of exfiltration, as described in my reports, on the laptop and I cite them and any independently veer -- any independent scientific qualified peer can look at the forensic image of the laptop in the same location and find the same exact evidence that I'm describing in my expert report.

Q. In your February 2023 declaration, you told the judge about the Digital Guardian report,

Page 98

right?

A. If it reference -- yes, it references the Digital Guardian report.

Q. And your declaration, like your report, never disclosed that the Digital Guardian report recorded no copying on January 8th, 2023, right?

A. If you're asking me does -- do any of my reports contain the sentence that I found no evidence of exfiltration within the Digital Guardian report itself, I don't believe they do.

I believe all of the evidence of exfiltration that I cite in my report exists on the laptop.

Q. And you went to a court hearing in March of 2023, right?

A. I did.

Q. You were prepared to testify at that hearing, right?

A. I was.

Q. Were you going to tell the judge that day that the Digital Guardian report did not show Grailer copying any files to her USB thumb drive on January 8th, 2023?

MR. YOSHIMURA: Objection.

Page 99

BY THE WITNESS:

A. If I was -- if I had been asked if the Digital Guardian report contained any evidence of exfiltration of files, I would have answered correctly and honestly the same way I did today; that I didn't find any evidence of exfiltration with the Digital Guardian report.

All the evidence of exfiltration I found all through forensic analysis of the laptop. All of the evidence is cited and can be independently verified and replicated by a qualified peer.

Q. Who prepared the Digital Guardian report?

A. I believe it was Jennifer Semmler, S-E-M-M-L-E-R.

Q. Do you know how she prepared it?

MR. YOSHIMURA: Objection.

BY THE WITNESS:

A. I do not.

Q. Have you ever personally generated a Digital Guardian report?

A. I have not.

Q. How many Digital Guardian reports have

Page 100

you analyzed during your career?

A. At least four different reports.

Q. When was the first one?

A. It was in the Ridley matter.

Q. And is one of the four in this Jessica Grailer matter?

A. Yes.

Q. What are the other two?

MR. YOSHIMURA: Objection.

BY THE WITNESS:

A. The other Ecolab matters.

Q. Okay. So all four Digital Guardian reports that you've analyzed have been in your Ecolab matters?

A. Correct.

Q. Have you received any training relating to Digital Guardian?

A. I have not.

Q. Have you received any training on how to interpret the data contained in a Digital Guardian report?

A. If you're asking me if I've gone through any sort of formal certification training process with the company Digital Guardian, I have

Page 101

not.

Q. Have you received informal training on how to interpret Digital Guardian reports?

A. So in my forensic analysis, in my career, since I've been doing this for 20 years, it is common on every case involving theft of trade secrets for me to collect and analyze business system logs such as Office 365 audit log, Digital Guardian's data loss prevention tool.

I actually have a CLE class that I -- called "Theft of Trade Secrets Best Practices." One of the slides recommends and suggests that it is important to preserve these sorts of logs as fast as humanly possible because that data is ephemeral in nature.

So I have experience -- extensive experience analyzing business logs, recording human interactions with files. And I've actually included that in a CLE class that I wrote and published.

Q. You have experience analyzing four Digital Guardian reports, correct?

A. Correct.

MR. YOSHIMURA: We've been going for a

Page 102

while. Is it okay to take a break?

MR. SPLITEK: Sure. Go right ahead.

THE VIDEOGRAPHER: The time is 11:14 a.m. We are going off the record.

(Whereupon, a break was taken, after which the following proceedings were had:)

THE VIDEOGRAPHER: The time is 11:30 a.m. and we are back on the record.

MR. SPLITEK: Mr. Lieb, I'm handing you Exhibit 9.

(Deposition Exhibit No. 9 was introduced to the witness.)

BY THE WITNESS:

A. Okay. And I understand that I'm still under oath.

Q. That's my understanding too.

A. Okay. Yes.

Q. And I will tell you Exhibit 9, these are screenshots. As you can see on page 1, you are getting rows 1 through 44, and then page 2 you're getting rows 45 through 77. And this is not intended to be filtered in any way. This is supposed to be a complete screenshot of a

Page 103

spreadsheet.

Having Exhibit 9 before you, Mr. Lieb, can you tell me what it is?

A. Yeah. This appears to be a true and exact copy of a file that was originally provided to me by Jennifer Semmler of Ecolab IT. The file name when it was originally provided to me was JGrailer.xlsx.

I have come to find out or through analysis that this is report actually is not a Digital Guardian report. This is an Office 365 audit log report.

And then this report was later supplemented with more rows and columns, more data after Ecolab restored backups from their Elastic audit log aggregation tool.

Q. So who first provided you with a log marked as Exhibit 9?

A. My recollection is it was Jessica -- I'm sorry, it was Jennifer Semmler, is my recollection.

Q. And when did she first provide you with a log marked as Exhibit 9?

A. I don't recall the specific date, but I

Page 104

believe it would have been sometime in February -- prior to the -- obviously prior to the publication of my original report.

Q. Okay. You received it before your February 2023 declaration?

A. Yes.

THE VIDEOGRAPHER: Hold on a second. The time is 11:33 a.m. We are going off the record.

(Whereupon, a discussion was had off the record.)

THE VIDEOGRAPHER: The time is 11:33 a.m. and we are back on the record.

MR. SPLITEK: Mr. Videographer, would you like the court reporter to read back the last question and answer?

THE VIDEOGRAPHER: Yes, please.

(Whereupon, the record was read as requested.)

BY MR. SPLITEK:

Q. Do you know who prepared the log marked as Exhibit 9?

A. My recollection is that this log Exhibit 9 was exported out of Ecolab's Elastic log

Page 105

aggregation tool.

Q. And do you know who handled that export?

A. My recollection, it was Jennifer Semmler.

Q. You were not personally involved in exporting the data shown in Exhibit 9?

A. I was not.

Q. And did you say that you later received a supplement to Exhibit 9?

A. I did.

Q. When did you receive that supplement?

A. It was around October of 2023, October/November 2023.

MR. SPLITEK: Okay. I'm going to share my screen again. I'm showing you Exhibit 10 on the screen, Mr. Lieb.

THE WITNESS: Okay.

(Deposition Exhibit No. 10 was introduced to the witness.)

BY MR. SPLITEK:

Q. In a moment -- so I'm showing it to you as we received it. In a moment I'm going to try to make it a little easier to read.

Page 106

But let me ask you so far: Do you recognize Exhibit 10 yet?

A. This appears to be the Office 365 audit log for Jessica Grailer that was restored from Ecolab's Elastic log aggregation tool.

Q. And then does Exhibit 10 also appear to be the supplement that you referred to earlier?

A. Is this Exhibit 10?

Q. Exhibit 10 is on the screen, yes.

A. Yes. Yes.

Q. Okay.

A. Correct.

Q. And I'm going to, just to make it a little easier here, I'm going to auto fit the column width.

A. Freeze the top row.

Q. I'm -- that's also a good idea.

First I'm going to make the row height a normal row height and also --

A. I think you have to hit the "enable edit."

Q. Ah-ha, thank you. That's why I can't. All right. So we will --

Okay. I'm going to back out. We're

Page 107

going to start over with Exhibit 10. You are correct, I need to enable editing first.

A. By the way, if you double click the line between A and B it will automatically spread them out. And then if you move it -- yeah, and double left click, it will do it -- there we go. And you can do the same thing with the rows between like -- yeah.

Q. All right. Very good. Thank you.

And so as we -- again, there is a lot of columns here.

A. Sorry to interrupt. If you don't mind freezing the top row, that will definitely aid in our analysis so we can see the column headers.

Q. Freeze top row.

A. Perfect.

Q. And, again, in Exhibit 10 like in Exhibit 4, there's -- there aren't as many rows but there's too many columns to make it manageable, but I'm scrolling through here.

And we see -- if we get to the bottom, it starts in the morning of January 8th, 2023; is that correct?

A. Yes.

Page 108

Q. Okay. And then it runs through, at the top, January 18th in the afternoon, correct?

A. That is correct.

Q. All right. And do you now -- do you recognize Exhibit 10 as that supplement that you received in October of 2023; is that right?

A. It is.

Q. Okay. So in your report you refer to an Office 365 user activity log, right?

A. Which exhibit are you referring to?

Q. Your report, Exhibit 2. And you can --

A. I have multiple reports.

Q. I understand. Let's just have you turn to Exhibit 2, paragraph 22.

A. Of exhibit -- sorry.

Q. Exhibit 2 of this deposition, paragraph 22.

A. Got it. Okay.

Q. Okay. Do you see you refer to an Office 365 user activity log there?

A. I do.

Q. So in that paragraph in Exhibit 2 of your report, are you talking about Exhibit 9 or Exhibit 10?

Page 109

A. In paragraph 2, if Exhibit 22 -- let's see. I have to read it.

Ecolab preserved Office 365 user activity log capturing the fact that a person, whom I assume to be Jessica Grailer, accessed her former Ecolab OneDrive account on January 11th, 2023; January 12th, 2023; January 13th, 2023; January 14th, 2023; January 15th, 2023; January 16th, 2023; January 17th, 2023; and January 18th, 2023 using an undisclosed computer. Jessica Grailer no longer had access to her Ecolab laptop as of January 10th, 2023, and, therefore, must have accessed her former Ecolab OneDrive account using an undisclosed computer.

I've included a true and exact copy of the log containing Jessica Grailer's activity as Exhibit E. So which -- is this -- is this Exhibit E or do I have a different exhibit?

Q. Let me back up a second here.

So in paragraph 2 -- in Exhibit 2, paragraph 22, you refer to -- you capitalize it -- "Office 365 user activity log."

Do you see that?

A. I do.

Page 110

Q. Okay. My question to you is: What are you referring to there?

A. It says: "I've included a true and exact copy of the log containing Jessica Grailer's activity as Exhibit E."

Q. That's right. But you didn't, right?

A. I didn't what?

Q. You did not include a true and correct copy of the log as Exhibit E to your report?

A. You're asserting that. I don't have a copy of Exhibit E.

Q. You do. It's in -- Exhibit 3 is all the exhibits to your report.

A. Exhibit 3?

Q. Yeah.

A. Okay.

Q. Look at Exhibit E.

A. Okay. I will.

Well, Exhibit E appears to be files exfiltrated by Grailer on January 8th. It doesn't appear to be the log.

Q. That's right.

And if you turn back in your report to paragraph 18 of your report; so this is paragraph

Page 111

18 of Exhibit 2.

A. Okay.

Q. You say there that Exhibit E is the list of files that you --

A. Okay. So paragraph 22, when I'm referring to the log, I must have missed that. It should have been Exhibit F. And Exhibit F should have been referred to as the JGrailer.xls report, which has more information, more columns and rows as what you're seeing as Lieb Exhibit 10.

So that's what I'm refer to in paragraph 2020 -- what I'm referring to in paragraph 22, the user activity log, I'm referring to it as the original JGrailer.xlsx file that was produced to me.

The subsequent expanded version that was recovered from the Elastic's system does not contain the information that contradicts or changes my opinions that I've stated in 22 or in my report. It just contains more columns and more detail.

Q. Okay. So to be clear, in paragraph 22 of your report, which we marked as Exhibit 2, when you refer to the Office 365 user activity log, you

Page 112

are referring to Exhibit 9; is that correct?

A. Yes.

Q. Okay. At some point did you analyze Exhibit 10 also?

A. Yes.

Q. Did you do that before or after preparing your report that's marked as Exhibit 2?

A. I'll have to look at production, when I produced this. I'm looking to see the date that I -- hopefully I put a date on here. Oh, November 13th.

I'd have to see the exact date that I got the restored expanded version which is your Exhibit 10. So as I'm sitting here, I don't recall because this is November 10th, 2023, which is right about the time I was provided with a new expanded audit log restored from Ecolab -- or from their Elastic system.

Q. And who first provided you with a log marked as Exhibit 10?

A. Exhibit 10?

Q. On the screen.

A. I don't recall.

Q. Do you remember how you received the

Page 113

log marked as Exhibit 10?

A. I don't.

Q. Do you remember whether it was someone from Ecolab or Fisher Phillips or the Faegre law firm?

A. I recall an Ecolab IT professional called Austin -- it's not Austin Powers -- it's Austin -- it's something like that. It's Austin Peters, something like that; was the gentleman at Ecolab IT who restored this Exhibit 10 from -- or actually had Elastic, the company, restore an archived backup and then provided this log.

I believe what you're asking me is how was that -- after it was generated by Austin after being restored by the company Elastic and how it was transmitted to me as like an e-mail attachment or uploaded to my share file, I don't recall.

Q. And do you know how anyone prepared the log marked as Exhibit 10?

A. Well, I was informed that Ecolab went to the company Elastic, who is this log aggregation software tool, and Elastic restored a backup archived that they had and was able to run this report, which is why we can see in some of

Page 114

the -- in your Exhibit 10 you can see some -- some columns are related to Elastic, this log aggregation tool, and some columns are directly from Microsoft.

Q. Did you ask for the log marked as Exhibit 10 or was it given to you without you're having to ask for it?

A. I don't recall.

Q. During the time you had the log marked as Exhibit 9 but not the log marked as Exhibit 10, did you ever feel that you were missing relevant information?

A. No.

Q. During that time did you ever ask anyone for additional information beyond what had been provided to you in the log marked as Exhibit 9?

A. I recall at the time asking Jennifer Semmler if there -- if there were -- was more data from the office -- the Office 365 audit log, and I believe that was in February of 2023, and she said this is the data.

So subsequent to that, conversations that I was not part of led to the company Elastic

Page 115

restoring the more thorough, more data, more rows and columns of this Office 365 audit log, which is now -- is my opinion is this Exhibit 10 on the screen.

Q. And have you received any training relating to logs like the ones marked as Exhibits 9 or 10?

A. I have not received formal Microsoft certification training, but I interact with Microsoft audit logs. I personally collect and generate those logs for some cases and clients. And I've done that at least 100 times and I describe that in the best practice of collecting such logs in my Theft and Trade Secrets Best Practice CLE class.

Q. Okay. So I'm going to bring down Exhibit 10.

A. Okay.

Q. And I'm going to focus on Exhibit 9 because that is the log you said you're identifying in paragraph 22 of your report.

A. Got it.

Q. Okay. So let's look at Exhibit 9.

A. Okay.

Page 116

Q. Do you see on both pages of Exhibit 9 there are "hard delete events"? The value is "hard delete" in the "Event" action column?

A. Yes.

Q. So what does a hard delete event mean to you?

A. Well, a hard delete -- so in Office 365 audit logs there -- and it doesn't show in these columns, but there's -- the most important type of deletion to record is what's known as a first-stage recycle bin and a second-stage recycle bin. So that is in terms of file.

So a first-stage recycle bin, that's the end user is moving date to just their normal Office 365 trash bin.

A second-stage recycle bin, means it's actually purged and no longer recoverable; this is according to Microsoft.

So I'd be speculating about what the "hard delete" is referred to. But I will note that my analysis of what you're referring to as Exhibit 10, if we look at those columns, the hard delete is calendar entries.

Q. Okay. And so let's break this down.

Page 117

So the hard delete events, what is being deleted is calendar entries; is that correct?

A. According to the Exhibit 10, yes.

Q. Okay. And to the best of your knowledge, that's what was being hard deleted, calendar entries?

A. Yes.

Q. Okay. And then you also talked about the first stage -- was it the first-stage recycle bin?

A. It's called a first-stage recycle bin and a second-stage recycle bin.

Q. And are you saying that the hard delete event represents, in this case, the calendar entries being permanently deleted from the second-stage recycle bin?

A. No. That's a good question.

So when I've encountered first-stage recycle bin entries and second-stage recycle bin entries in Office 365 audit logs, that's been in reference to files and folders. So I would have to research it to answer that question.

So the hard delete may specifically refer to Outlook calendar entries instead of

Page 118

individual files like PDF files.

Q. Okay. When -- I thought you did say that it refers to calendar entries in this instance.

A. It does.

Q. Okay. When a calendar entry is being hard deleted, what is happening to it?

A. I don't know what the designation of hard delete means beyond deletion of that entry.

Q. Okay. And do you know whether the hard delete event for a calendar entry reflects a user's action or the calendar entry being purged from the recoverable items folder after being soft deleted earlier?

A. In my opinion, these entries in Exhibit 9 that state hard delete were performed by Jessica Grailer.

Q. And why do you think that?

A. In the expanded Exhibit 10 we can see the user account says Jessica Grailer.

Q. All right. Any other reason?

A. I've never encountered any instance where a direct user account access password has ever been provided to another employee. That

Page 119

would not be best practice. I've never seen that done.

So, in other words, if another user had deleted these calendar entries, it would show up in their audit log under not JGrailer@Ecolab; it would show up under somebody else's account.

Q. Well, that wasn't quite my question.

Is it -- does a Microsoft audit log ever record events that no user initiated such as an automatic purge of items from the recoverable items folder?

A. I don't have any experience encountering that in my analysis so I can't answer that. It is not in my experience.

Q. Take a look at the user login failed events that we see in both page 1 and page 2 of Exhibit 9. What are those showing us?

A. Those are showing that Jessica Grailer attempting to log in. So, for example, row 13, Exhibit 9, says "user login failed." So outcome failure. Has an IP address 131.95.104.251, my research showed that to be Charter Communications, consumer -- consumer Internet account.

I asked Ecolab IT if they used Charter

Page 120

Communications in any capacity; they said no.

So my opinion, this is Jessica Grailer's home Internet and it shows that it was done by -- she used a -- under "User Agent", column F, an Apple iPhone. It says 13C1. That actually is actually an iPhone 12 mini, slash, 2003.85. That 2003.85 refers to the operating system version of her iPhone 12 mini.

And if we look at Exhibit 10, which has even more columns, it says the reason for the user login failure, it says "user error."

Q. And did you do any analysis to determine whether an application installed on Grailer's iPhone could have initiated that failed user login event without Grailer's intervention?

A. I was not provided with a forensic image of Ms. Grailer's iPhone 12 mini so I can't opine as to what evidence exists on the iPhone 12 mini. I was not provided with that.

But it is my opinion that Jessica Grailer attempted to log in to her former Ecolab work account on multiple days, as recorded in this log, attempted to and failed using her iPhone 12 mini.

Page 121

Q. And in those events, she did -- in any event, she did not gain access to her account; is that correct?

A. Well, she didn't access -- according to these logs, she didn't gain access using her iPhone 12 mini. It said "login failure."

Q. So, for example, in row 43 at 52 minutes after midnight on January 14th --

A. Sorry, are you on the second page? You said row --

Q. First page of Exhibit 9, row 43.

A. Oh, 43. Sorry. Yes, user login failed, event outcome failure. Shows the source IP address. And then it, again, shows it is her iPhone 12 mini.

Q. But that's an example of Grailer not gaining access to her account at 12:52 a.m. on January 14th, correct?

A. Correct. All of the entries captured in Exhibit 9 that relate to her iPhone 12 mini show that she was not successful; that her user login failed or she failed to log in into her former work account user her iPhone 12 mini.

Q. But in your February 2023 declaration

Page 122

you testified that Grailer did access her account at that exact date and time, didn't you?

A. She attempted to access her account. This is accessing her account. Her login failed but she did access her account. So I mean, she went to the house to go into it, knocked on the door, it was locked. Her key didn't work.

So to me that's her attempting to enter the house. That's what I mean by access.

Q. So when you testified in your declaration that Jessica Grailer accessed her Ecolab OneDrive account on January 14th, 2023, at 52 minutes after midnight you meant that she tried to login but failed to do it?

A. That's -- that's what the evidence shows.

Q. There are a series of filed previewed events on page 1 of Exhibit 9.

A. Yes, I see those.

Q. What does a "file previewed event" mean to you?

A. In my opinion that means interaction with those files.

Q. Well, that's really vague. What kind

Page 123

of interaction?

A. In my opinion, and the evidence is consistent with Jessica Grailer using an undisclosed computer to access her former work accounts on these dates, access these files and she is in possession of those files.

Q. But I don't -- it still is pretty vague.

What do you mean by access the files and be in possession of them? On the page it just says "file previewed," right?

A. Right.

Q. So tell me as precise as you can, what do you think happened at 1:01 p.m. on January 15th to result in these file previewed events in the log?

A. Right. So if we look at the timestamps -- again, this is in rapid succession. So in my opinion, she used an undisclosed device, successfully accessed and logged into her former work account and took exfiltrated copies of all of these files.

It's my opinion that a forensic analysis of this undisclosed device, potentially

Page 124

her new Chem Tree laptop, her Emtec USB drive would show evidence of these files existing on those devices.

Q. How did she exfiltrate them? I don't understand. Logistically.

A. Downloaded.

Q. So the file previewed events that we see in Exhibit 9, you're saying that she accessed the files and downloaded the files; is that right?

A. In my opinion, this evidence is consistent with a person, I believe to be Jessica Grailer, accessing her former work account using an undisclosed computer device, and then in rapid succession accessing all of these files and downloading them, taking a copy of them.

Q. So you're saying --

A. Sorry, go ahead.

Q. So you're saying that when someone accesses and downloads files, what results are entries in the log that say "file previewed"?

A. Yes. It says "file previewed" but you'll notice that the timestamps are within two seconds of each other. So, again, a human being, just as we saw with evidence on her laptop, a

Page 125

human being is not opening up -- I don't believe -- it is not my opinion that Jessica Grailer opened up these dozen-plus files within seconds -- within microseconds of each other.

It's, in many opinion, the evidence is consistent with the fact that she successfully accessed her account using an undisclosed device on that date and then accessed these files to take them, and she did.

And my opinion is that a forensic analysis of her -- this undisclosed computer, the Emtec USB drive and her new Chem Tree work computer e-mail account, new Chem Tree OneDrive would show evidence of these files existing in those locations, one or more of these locations, and information derived from these files.

Q. Did you look up who owns the IP address that shows up in column D next to the "file previewed" events on page 1 of Exhibit 9?

A. I did.

Q. And who owns it?

A. Microsoft.

Q. In paragraph 30 of your report --

A. Which exhibit?

Page 126

Q. Exhibit 2.

A. I'm there.

Q. -- you say that [as read]: The Ecolab OneDrive log shows that Jessica Grailer successfully logged in and opened and deleted files on multiple dates after her resignation on January 8th, 2023.

A. I see that.

Q. Right?

So which -- well, let's break it down.

Which rows in Exhibit 9 show Grailer successfully logging into her account?

A. So -- well -- okay.

So the fact that she was able to interact with files, preview them, download them in my opinion, the fact that she was able to delete entries -- now -- and at the time I wrote paragraph 30 in February of 2023, I was not -- I did not have access to what you're Exhibit 10 is, the expanded. That actually showed the column of what the hard delete was, that it was calendar events.

So paragraph 3, it said deleted files on multiple dates. Now that I have access

Page 127

subsequent to that with your Exhibit 10, it actually shows they were not PDF files or Word files. They were actually calendar entries that she deleted.

Q. All right. I want to be clear, though.

I'm looking at Exhibit 2, paragraph 30.

A. Right.

Q. It's your November report. Are you in Exhibit 2?

A. Okay, I'm there.

Q. Paragraph 30. You say that [as read]: The OneDrive log shows that Jessica Grailer successfully logged in and opened and deleted files on multiple dates.

A. Okay.

Q. But you're saying now it's calendar entries; it's not files?

A. I mean, clearly Exhibit 10 -- again, as I sit here, when I looked at 30, I may have been referring to your Exhibit 9, which doesn't have the columns for what was specifically hard deleted.

Your Exhibit 10, it does have the columns so we can see that it was calendar entries

Page 128

that were deleted.

Q. Okay. And which rows in Exhibit 9, again, show Grailer logging in successfully?

A. I don't see any entries for user login success. But clearly she must have successfully logged in because the activities that -- well, it is in Exhibit 10, it shows that the user account that was performing these activities in Exhibit 9 are all under the J. Grailer account.

So, therefore, she must have been able to login successfully to perform actions that were recorded by Office 365.

Q. But how did she manage to log in without generating a user logged-in event in the log?

A. I don't know why this audit log doesn't record the login success.

Q. Okay. But that's what you're say is the log just -- it doesn't record when users log in?

A. This log doesn't contain -- neither Exhibit 9 nor Exhibit 10, as far as I can tell -- you'd have to look at Exhibit 10 to see if there is a login success entry.

Page 129

Q. Okay.

A. You can go data and search for that and see if there's a login success entry. I don't recall one.

But the fact that on Exhibit 10 we can see these activities were performed by the user account JGrailer@Ecolab.com. So in my opinion, that's Jessica Grailer.

Q. And it looks like, for whatever reason, it looks like to you that the log just wasn't recording when there was a successful login. It was only recording when there was a failed login; is that right?

A. Yes.

Q. Okay.

A. And in Exhibit 10 -- I don't have Exhibit 10 in front of me, but if you brought it back up we might be able to sort the event action outcome to see if the expanded log actually has a login success. It may. I don't recall.

Q. Yeah. You think there is not one in there, I take it?

A. I don't recall.

Q. Which rows in Exhibit 9 show Grailer

Page 130

opening any files?

A. Well, it is rows 22 through 41, which show the files that I described, I believe in multiple declarations.

So in my Exhibit 2 it is table 1, files accessed by Jessica Grailer on January 15th.

Q. I'm going to cut you off.

In Exhibit 9, which rows in Exhibit 9 show Grailer opening any files?

A. Well, I see her accessing and downloading and exfiltrating the files. It is my opinion that she opened, accessed, downloaded these files that are listed in Exhibit 9 in rows 22 through 41.

Q. Okay. But you're saying that you believe rows 22 through 41 of Exhibit 9 show Grailer opening the files that are listed?

A. It is any opinion that Jessica Grailer accessed, opened, downloaded, has a copy -- exfiltrated these files. It is -- again, in your Exhibit 10 it shows it was done by the Jessica Grailer account.

It is my opinion that that is Jessica Grailer surreptitiously accessing her former work

Page 131

account and exfiltrating these files using an undisclosed computer. I'd like her to explain why or what device she used. Did she explain to anyone what device she was using?

MR. YOSHIMURA: Larry, you don't ask questions.

THE WITNESS: I know. Sorry.

MR. SPLITEK: All right. I'm going to hand you Exhibit 11.

(Deposition Exhibit No. 11 was introduced to the witness.)

BY THE WITNESS:

A. Okay.

Q. And you'll be able to verify this for yourself, if you would like later, but Exhibit 11 are screenshots showing not all of the columns because, as we saw, there is a lot of columns, but some of the columns for all of the earliest records --

A. Okay.

Q. -- from the log that we marked as Exhibit 10.

MR. YOSHIMURA: Are these row numbers going to match up?

Page 132

MR. SPLITEK: These row numbers are going to match up because you can't sort Exhibit 10 as easily because of the way that they have formatted the timestamp.

BY THE WITNESS:

A. Okay.

Q. All right. So these are the earliest records, and so the earliest record begins at 10:51 a.m. on January 8th, and then on this Exhibit 11, the latest record is 8:12 p.m. on January 8th.

There are, of course, many other records in Exhibit 10, right?

A. There are.

Q. And then the way, just to make sure we're all clear on this, each page of Exhibit 11 shows different columns for the same rows. So if you look, each page of Exhibit 11 is the same rows 393 through 435. And as you turn through the pages, you get more and more columns relating to those rows.

A. I understand.

Q. Okay?

A. Yes.

Page 133

Q. So I want to just talk through a couple of these by -- as examples so you can help me understand how you're approaching this.

A. I would note that on your Exhibit 11 the first page, row 433, it says "user logged in."

Q. Yes. I actually want to ask you about row 433.

So column Y. The event action column, it says "user logged in."

A. Yes.

Q. So what does that mean to you?

A. It means that Jessica Grailer logged into her account.

Q. Okay. And how did Jessica Grailer, in your view, log in to her account after January 8th, 2023, without generating a user logged-in event in the log?

A. I don't know why the -- well, it is interesting. So if we look at -- if we look at column GP on the last page, right, we can see rows 409, 410, 411, it has references to an HP EliteBook X360, which is consistent with the make and model of her former work laptop.

So the row where you're saying where it

Page 134

says "login," it just references a -- it says AppleWebKit, Chrome. So it doesn't reference a device. So -- well, it says "user agent OS name," it says "Windows." So it's a Windows device, according to this log.

But it doesn't -- unfortunately it doesn't have a -- when it says user logged in, it doesn't have, in column GP, it doesn't have reference to a device.

Q. Yeah. But that really wasn't my question.

So you agree that Jessica Grailer logged into her account on January 8th, 2023, right?

A. That's what the log shows and, yes, that's what is consistent with what this log shows.

Q. And when she logged in, it generated a user logged-in event in the log, right?

A. It did.

Q. So my question is: How could Grailer have later logged in without generating any user logged-in events?

A. So it is a good question. I looked at

Page 135

this closely. So because there is not a -- there's not any indication of what device was used to log in on the 8th, my current opinion is that she logged in successfully using this undisclosed device, and then she may have stayed logged in. That would be a reasonable explanation.

Q. She logged in when and stayed logged in?

A. Well, it says -- so we have on January 8th, it says "user login success."

Again, we don't have any indication from this Office 365 log what specific device she used to log in, but I don't see any log out. There is user login. I don't see any log out.

Q. I agree. I don't see those either.

A. Let me look at row 406.

Q. Are you saying that Jessica Grailer logged in on January 8th, 2023, and then stayed logged in through January 15th, 2023?

A. Yeah, that's a reasonable explanation; that once the device is logged in, unless she, like, logs out, it would remain logged in. So, again, like -- I'm looking at row 406, which is another user logged-in action, but unfortunately

Page 136

it doesn't show a device was used. It just shows it was a Windows -- it just shows Windows authentication provider 10 Windows. So it doesn't show.

So if you're asking why in the exhibit the larger -- well, the expanded exhibit, so the surreptitious -- what I'm describing as surreptitious activity and access and exfiltration of files, why it doesn't -- none of the logs show the specific device.

That's why, in my expert report, I don't say, oh, she used a -- an undisclosed device is a Windows machine or it's an iPad. The logs don't show that so I'm not going to make it up.

But clearly it shows Jessica Grailer user account performing this interaction that I describe in my reports because it is under the JGrailer@Ecolab.com.

She returned her work laptop and her iPhone 6S and iPhone XR -- it says, I have the chain of custody, January 10th. She no longer had custody and control over her work HP EliteBook or her iPhone 6S and her iPhone XR.

On the later dates, the later dates I

Page 137

described after January 8th, we see in a log there is evidence that she was not successfully able to log in using her iPhone 12 mini but that on other dates she was able to interact with files including, in my opinion, evidence of the exfiltration of the files that exist in Exhibit 9.

So which, again, in my opinion, it falls on Ms. Grailer to explain what device she was able to use to perform these interactions.

Q. I want to make sure we're clear here.

So you're claim is that she logged in sometime on January 8th, 2023, using an undisclosed computer and stayed logged in through January 15th, 2023; is that correct?

A. I know you're not intentionally mischaracterizing what I said so let me respond. I know you're not, unlike other attorneys I've encountered. I appreciate you're not doing that.

So in here it says, "user logged in." I don't see any reference in your Exhibit 10 to what device was used to log in. It says she was logged in.

Q. I know. I'm going to cut you off because it's just not my question.

Page 138

I'm asking you -- and I'm not trying to characterize --

A. I'm answering your question. You mischaracterized what I said.

Q. But my question is about a claim.

A. Okay, sorry.

Q. But I'm just asking you -- it's yes or no -- are you claiming that Jessica Grailer logged in using some undisclosed computer on January 8th, 2023, and stayed logged in through January 15th, 2023?

A. No.

What I'm stating is that this expanded Exhibit 10 or what you show as also Exhibit 11 which encompasses the information, shows that a successful login by Ms. Grailer. It doesn't show what device was used. We can just see it's a Windows operating system. It doesn't say which -- I noted it doesn't refer to her EliteBook, right? Because that would be my opinion, that she used the EliteBook.

So -- I'm sorry. So the activity that we see after January 8th, that obviously she was using a device that was logged in. If she

Page 139

couldn't log in -- if she was not logged in she would not have been able to interact with -- perform the interactions that are recorded in the log.

So the best explanation I have is that a device --an undisclosed computing device had successfully logged in prior and we don't see that login because the -- and she used that device.

She had to have been able to access her account. She was able to access her account. It says the iPhone 12 mini was failed, but it clearly shows that she was able to interact with these files, in my opinion, exfiltrating the files listed, deleting these calendar entries. I have no idea why she would delete calendar entries, but using an undisclosed device.

To be clear, none of the audit logs refer to what device it was, which is why I describe it as an undisclosed device. If I knew specifically what it was, I would say what it was. I don't know. That's why one would have to ask Ms. Grailer what device she used to perform these interactions.

Q. Let me ask you this a different way,

Page 140

though. Somewhere in the log there is a -- the user logged-in event, that later enabled Grailer to perform the activities that you said she performed on January 15th, correct?

A. So I don't know if you're asking this. But it could have been a device that -- you're asking me to speculate. So it could have been a device that -- this log doesn't go back to January 1st. So could that be that she's using this undisclosed computer and logged in January 1st or late December and just stayed logged in. There's no reason for her to log out.

And so we don't -- but, obviously, she had to have been logged in to her account under her JGrailer account to perform the activities that the log --

Q. Let me ask it -- back up and ask a slightly different question.

If Grailer used an undisclosed computer to log into her account --

A. Okay.

Q. -- and then on January 15th exfiltrate files, at some point before January 15th, whatever day it would have been on, whether it is shown in

Page 141

the logs we have or not, there would have been a Microsoft audit log entry showing the login event from her undisclosed computer?

A. I would assume so, yes, that would be my opinion.

Q. Okay.

A. And to further answer, we see user logged-in entries on January 8th but, unfortunately, it doesn't specify what device it -- but it does say Windows operating system. It doesn't say the -- it even has a little bit more information. It says it was a Safari browser.

Q. And you, I take it, didn't try to find the login event that you believe later enabled her to exfiltrate files on January 15th?

A. Well, I analyzed the user audit logs the first one that was provided to me, we'll call it the truncated one, and then the subsequent, I believe it's your Exhibit 10, that had more columns, I looked at that very closely.

Q. But that wasn't my question.

My question is: You didn't try to find the user logged-in event that you're now saying enabled to Grailer to exfiltrate files on January

Page 142

15th?

MR. YOSHIMURA: Objection.

BY THE WITNESS:

A. So I analyzed these logs to identify evidence of what this undisclosed computer was; make, model, entries. I didn't find it in Exhibit 11 or the expanded, the restored Elastic log. I only see reference to this HP EliteBook X360 and the iPhone 12 mini.

And as I stated earlier, in this exhibit -- your Exhibit 11, we see user logged-in activities, but it doesn't list what device was used, unfortunately.

Q. In column AA, in row 433, what do you believe -- sorry, I apologize. We're still in Exhibit 11 to make sure.

A. I'm here.

Q. Exhibit 11, row 433, column AA, event category. What do you believe the terms "web" and "authentication" are telling us?

A. So my understanding is that in order to -- for an employee of Ecolab to successfully access an Ecolab company system, that device has to be authenticated as a security measure by

Page 143

Ecolab's IT.

So the authentication, in my opinion, is showing that Ecolab said, okay, this is an approved -- for lack of a better term, an approved device. It's a security measure so that some hacker, you know, can't log into -- that's why, in my opinion, the iPhone 12 mini was blocked.

I don't know. I'd be happy to be informed as to what the purchase date of her iPhone 12 mini was, but I don't see any other earlier access of her accounts or attempts to access with her account.

If she had earlier and that device had been approved by Ecolab, I think she would have been able to successfully log in using that iPhone 12 mini. But the evidence I see here shows that after she left employment she attempted to access her accounts using her iPhone 12 mini, including from what I believe to be her home network, and it was blocked.

Q. And what does the term "web" tell us in column AA, row 433 in Exhibit 11?

A. Well, it says "web authentication." So if we look at --

Page 144

Q. But I'm asking about web. Just tell me about web. What does it mean to you there?

A. I believe it's related to the type of access that she was using, like an Internet browser. So if we see, for example, in column -- the next column says "OS browser, browser type is compliant and managed."

Q. All right. And then in column AJ, the event type column, still in row 433, what does the term "info" mean to you there?

A. Which page?

Q. Page 1 of Exhibit 11, row 433, column AJ?

A. Oh, "info"?

Q. The first word is "info." Why is that there, in your view?

A. I don't know what that means.

Q. Okay. Then the next word is "start." Why is "start" there, in your view?

A. I don't know what "start" or "access" means.

Q. Okay. Column -- so page 2 of Exhibit 11, still in row 433. Let's take a look at column FV, source is organization name?

Page 145

A. Yes.

Q. Z-S caler?

A. Zscaler.

Q. Thanks. Do you recognize that? What is Zscaler-SJC1?

A. I recall that my analysis of the IP address, I believe that is an IP. I believe it is Verizon business.

Q. So what is it? What are we learning here in column FV?

A. I believe it is -- I believe it's reference to the ISP or the Internet service provider that she used. As part of -- my recollection is part of the -- part of -- as part of the corpus of evidence that was provided to me at the outset of this engagement, I was provided with a wireless hotspot, and my recollection it was a Verizon device.

And so, again, in my analysis of the device I tracked down what these different IP address, which Internet provider, Internet service provider these relate to. That's how I know the starting one, 131 is Charter Communications. The other ones we see is Microsoft themselves. And I

Page 146

believe the Zscaler is -- I don't have my own version of this file where I -- you know, I created another tab where I took out each of the IP addresses and looked up what ISP they relate to.

I believe Zscaler relates to Verizon Wireless, which would be consistent with the fact that she had a Verizon Wireless hotspot.

Q. Verizon Wireless hotspot provided by --

A. Ecolab.

Q. -- Ecolab?

A. Correct.

Q. And then in columns FX and GE, still in the second page of Exhibit 11 --

A. I'm in.

Q. -- we see Chicago and then an IP address?

A. Yes.

Q. How do you explain those?

A. Again, my recollection is that Zscaler Chicago in this IP address correlates to Verizon Wireless.

Q. To the hotspot she received from Ecolab?

Page 147

A. I was provided with a Verizon Wireless hotspot. I looked up this IP address using one of my tools. It said that this IP address is owned by Verizon Wireless. I don't know why it says Zscaler. But in my opinion -- again, my recollection is that these are actually Verizon Wireless, owned by Verizon Wireless, which would make sense given the fact that she had a Verizon hotspot.

Q. And then column GP and GT on the last page of Exhibit 11.

A. I'm there.

Q. What are these telling us together?

A. These actually show the application being used in some instances. So we'll see like going from the top it says Microsoft Excel, the version, it was a Windows 10 machine. It was a desktop application. And then we can see the HP EliteBook X360 1030.

Q. And let's focus on row 433 in columns GP and GT.

A. Yep.

Q. And I know you talked a little bit about that before. But what then --

Page 148

A. So 433 shows that it was -- this activity was performed using a -- using the Mozilla Firefox browser. It says AppleWebKit, but my interpretation is that it's Windows -- it's Windows -- not Windows. Sorry. It is actually the Mozilla browser. Then it says Chrome. So it's kind of contrary. It says Mozilla and Chrome. Chrome is made by Google. And then it says Safari, which is an Apple browser. And then it says Edge. So -- and then it says operating system is Windows.

So I don't have an explanation as to why the user agent has Mozilla Firefox, AppleWebKit, which would relate to the Safari browser, Google Chrome browser and Microsoft Edge browser, all three. I don't want to speculate why all three are listed in there. It doesn't list the device that was used.

Q. Let's go back to the first page of Exhibit 11. And I want to look at row 417 now.

A. Okay. I'm there.

Q. In column Y, what does the term "file accessed" mean to you in column Y, row 417 of Exhibit 11?

Page 149

A. Means that she accessed a file.

Q. Okay. And how, though, on January 15th, do you think she was able to access files without generating any file accessed events in the log?

A. I don't want to opine as to what this specific difference between file access and file previewed is. But in my opinion, that is evidence of human interaction and is consistent with, again, my opinion, that Jessica Grailer used an undisclosed computer or January 15th to exfiltrate multiple files.

Q. But you don't have an opinion on what the difference is between a file-accessed event like we're seeing in Exhibit 11 and the file-previewed events that happened on January 15th, right?

A. I do not.

Q. Okay. Column AA, still in Exhibit 11, row 417.

A. Okay.

Q. Column AA. We already talked about the term "web" earlier.

A. Okay.

Page 150

Q. But there is another term here, "file." What does "file" mean to you there in 417, column AA in Exhibit 11?

A. I don't know.

Q. All right.

A. Some say "web," some say "web, file," some say "web, authentication." I don't know what the distinction is.

Q. Okay. So Exhibit 11, row 417, column AJ, the event provider column, that says "OneDrive."

A. Okay.

Q. What is that telling us?

A. That tells me that, in my opinion, Ms. Grailer was interacting with files stored in her OneDrive account. Although, I will note that, as I look at the other columns in this exhibit -- do you have a listing of what the file -- yeah, we do see that. We see in column -- sorry.

Q. Is it column GG?

A. Yes. Exactly, right. GG, then we see it actually is referring to -- yeah, there is actual file names.

Q. Okay. And so in column GG, let's take

Page 151

row 417, for example.

A. Okay.

Q. It says -- after the HTTP, there's Ecolab-my.sharepoint.com/personal. In here it's JA Galliart. But that, my.sharepoint.com/personal, is that what is telling us that we're in an employee's OneDrive folders?

A. So the way SharePoint works is an employee will create a file. They'll be the owner of that file. It will be stored obviously in their own OneDrive account. And if they give access to that other employees, the other employees will think that file exists in their OneDrive account. But it's really a pointer to it.

So what this entry shows me is that this file that Ms. Grailer was accessing, like the actual underlying file, what's in shared folders is originated from Josh Galliart.

Q. From his OneDrive?

A. Right.

Q. Okay. And then in row 418 just below in column GG, that's in a J Grailer OneDrive

Page 152

folder, right?

A. Yes.

Q. Okay. And you can tell that it's their personal OneDrive folders because it says my.Sharepoint.com/personal and then the employee's name, right?

A. Yes.

Q. Okay. Got it.

I need to clarify something for the record because I think I made a misstatement due to bad vision. We talked about just a moment ago on page 1 of Exhibit 11 the event provider column. I believe I said it was column AJ. It is actually AI.

Do you agree?

A. Yes.

Q. Okay. Sorry for that. I'm getting old.

What is the difference between OneDrive and SharePoint?

A. Well, OneDrive -- OneDrive is used for what's known as personal or home directory. So each employee would be provided with their own personal OneDrive account. So OneDrive, they're

Page 153

file cabinets, right? So it is their file cabinet.

SharePoint -- SharePoint is Microsoft's reference to files that can be accessed by more than one person. But, again, it is really critical to understand that SharePoint is a database with pointers to files.

So there might be an occasion where there is a unique file that was created in share file -- I don't believe that. I may have encountered that. Generally speaking, it's files that are created by employees, created and stored in their OneDrive accounts.

And as they're shared to other employees, the other employee thinks it's in their account but it's really just a pointer and they can download and access and open it. But when we go to do forensic collections of employee's accounts, we collect their OneDrive accounts.

In some instances there is what's known as share departmental folders in SharePoint. It would be like a sales department or an accounting department, right, not tied to a single employee and we can download specific SharePoint

Page 154

directories. But, in general, the best practice is to download and preserve the employee's OneDrive account because that is actually going to grab the files that we're interested in.

Q. In the last page of Exhibit 11 in column GP --

A. Okay. I'm there.

Q. I apologize. On Exhibit 11, page 3 in column GG in both row 417 and row 418, we saw file paths going into employees' personal OneDrive folders, right?

A. Yes. Says: My.sharepoint.com/personal and J Grailer, and one above it shows Josh Galliart and then Aaron Beranek.

Q. And then if we turn back to the first page of Exhibit 11, column, AI, the event provider column, that confirms this is an event in OneDrive, correct?

A. Right.

Q. Okay. Now we can go to the last page of Exhibit 11.

A. Okay.

Q. And let's stick with row 417 here.

A. Okay.

Page 155

Q. Column GP. That column identifies Grailer's work laptop, right?

A. Yes. But the only caveat I would say is that I was provided with an HP EliteBook X3630 reported to be Jessica Grailer's, but this doesn't have a serial number tied to it. So I'm assuming she was using her own HP EliteBook that X360.

If I perform forensic analysis of the Axiom database, I could say, oh, you know, I see on this date and time this Internet activity. I have not done that. So more likely than not this HP EliteBook X360 is referring to her former work laptop.

Q. Okay. In any event, it records the device that she was using when she accessed a file, right?

A. It does.

Q. Okay. And in column GT it also records the operating system of the device she was using, right?

A. It does.

Q. Okay. So how then on January 15th could she successfully access files without leaving any trace of the device or the operating

Page 156

system she was using?

A. Well, we would have to see the -- I think it was your Exhibit 10 for those rows. I don't know if you can bring that up on the screen but that's what we would want -- we would want to look at the equivalent, whatever row GP and --

Q. You would expect that --

A. For me to be able to answer --

Q. -- then you would see the device there?

A. Well, I don't know. I don't know. I don't have that Exhibit 10 memorized.

Q. I'm not asking what's in it. I'm asking you what you would expect.

If an employee accesses files from a computer and the computer is running an operating system, we see here in columns GP and GT of Exhibit 11 that the audit log made a record of the device and operating system that Grailer was using for the access event shown in row 417 in Exhibit 11, right?

A. Yeah. But I note the difference in the -- in your Exhibit 11 it shows in column GG URL original which is, you know, the equivalent of a website URL, but it doesn't have the column file

Page 157

name. I don't know why.

Q. I'm sorry, what column are we looking at?

A. Sorry. GG.

Q. GG?

A. Yeah, it says URL, U-R-L, original.

Q. Yes. I'm not looking at column GG, so I want you to look at -- maybe I misspoke -- Exhibit 11, last page.

A. Okay.

Q. Column GP. In row 417.

A. Okay.

Q. The log made a record of the computer device that Grailer was using when she accessed the file, right?

A. Right. 417, using Microsoft Excel.

Q. Yep. And then in addition to column GT, the log made a record of the operating system running on the computer that Grailer was using when she accessed a file, correct?

A. It does, yeah.

Q. Okay. Would you expect the log to make similar records regarding the computer and the operating system she would have been using to

Page 158

access files on January 15th?

A. I don't know. The answer lies in Exhibit 10.

Q. No, it doesn't. Because that is a question about what is in Exhibit 10. And my question is, what would you expect to see?

MR. YOSHIMURA: Matt, I think you have to give him an opportunity to answer the question. And now, objection; asked and answered.

BY THE WITNESS:

A. I don't have Exhibit 10 in front of me, so I don't have it memorized so I'm not going to speculate as to what I can't remember or have in front of me. Because it is like hundreds and hundreds of rows. So whatever that is showing is what the evidence that was recorded.

Q. But, again, I'm not asking you about what is in Exhibit 10. Let me ask a more general question.

When an employee like Grailer accesses a file from a computer, would you expect the log to make a record of the device that the employee was using?

Page 159

A. Well, I don't know because I'm looking at row 423 of Exhibit 11 which shows file preview, web OneDrive, and if I go to the last page on 423 it doesn't list the device.

So for file preview it doesn't -- for that row at least it doesn't list the device that was used to preview that file. It just lists that it was done, OneDrive, and then 1.0. So it doesn't list the device.

Q. It does list a user agent, though, correct?

A. For 423?

Q. The field is not blank?

A. 423, user agent would be -- which column? Which page?

Q. Column GP.

A. GP. Sorry. 423. GP, row 423 says OneDrive -- transform thumbnail 1.0. I don't think of OneDrive as an application.

So if you're asking if that user agent is an application, I think of OneDrive as a file storage source, not an application, per se, like an Internet browser or a Microsoft Excel.

Q. Have you ever -- do you have any

Page 160

experience with that terminology that we're seeing there, OneDriveMPC-transform_thumbnail? Does that mean anything to you?

A. It does not.

Q. You've never reviewed any materials that Microsoft might make available relating to that term?

A. I have not researched what that term specifically refers to.

Q. All right. Do you know if nonuser activities can generate any log entries in a log relating to a user's account?

A. So the way I'll answer that is when I personally collect and generate Office 365 audit logs from Microsoft, what used to be known as their compliance center, they call it something different now, the available fields columns that one can export, there is hundreds and hundreds of them. And so I -- personally I limit the fields I export to human interaction.

So I believe my recollection is that there are fields that are -- that would be system related, system generated, nonhuman related. I don't recall. I'd have to see. I can log into my

Page 161

own Tyger Forensics 365 compliance center, run the user audit log and you can see in the drop-down, it's like a crazy number of columns that can be exported.

But I personally historically limit what I export in reports to fields and columns that directly tied to human activity because that's what -- my opinion would only be what's only relevant to dispute resolution.

Q. I'm handing you Exhibit 12.

A. Okay.

MR. YOSHIMURA: Matt, if this one is going to take the same amount of time as the last one, I'd make a suggestion we break for lunch before we do this one or after?

MR. SPLITEK: Why don't we do this exhibit. I've already handed it to you, so ...

MR. YOSHIMURA: All right.

(Deposition Exhibit No. 12 was introduced to the witness.)

BY MR. SPLITEK:

Q. I will tell you, Exhibit 12 is more information about events that are shown in the log

Page 162

marked as Exhibit 10. It captures rows 21 through 64 and that spans the entire time period between January 13 and January 16 of 2023. And then, again, there are select columns similar to Exhibit 11.

Do you understand?

A. Yes. I'm noting that there is -- yeah, not all columns are obviously visible because it goes from column A to column Y, so columns B through X are hidden, in my opinion. Not all the rows are visible because it goes from 1 to 21.

So it goes through -- is row 21, is that January 17th?

Q. Yes.

A. So then it goes 17, 16. So there's nothing for January 18th in this.

Q. On Exhibit 12.

A. On Exhibit 12.

Q. There is in Exhibit 10. But Exhibit 12 is a screenshot of only a certain time range.

A. So it's specific -- it's specific rows and columns that you have made visible from the total corpus.

Q. That is correct. And it captures the

Page 163

entire January 13 through January 16th time period.

A. Well, plus January 17th.

Q. And it also captures little parts of the 17th and the 12th, that's correct.

A. Okay.

Q. Okay. So let's focus in on rows 31 through 50. I think we've already talked about some of this data when it was in the smaller log marked as Exhibit 9, right?

A. Uh-huh.

Q. So in column AA, event category, do you make anything of the fact that it says only "web" and never "file" in rows 3150, column AA?

A. I do not. It says file previewed --

Q. No, column AA.

A. It says web. Interesting. Column DM says "is a managed device," it says "false." Interesting.

Q. I'm asking about column AA. It says only "web."

A. Yeah.

Q. It never says "file." So I'm asking you, do you make anything of that fact, that it

Page 164

never says "file" in that column?

A. Well, what I'm making is column M shows that it's not a managed device.

Q. I'm not asking about column M.

A. Well, I'm answering that the exhibit you showed me shows that all these files that my opinions she exfiltrated, it shows it was from a device that was not -- says "audit is not managed."

It does show that it was file previewed. It shows web. I don't see the web file.

MR. YOSHIMURA: Larry, if you'd avoid crosstalk on the record. Please let him finish his question and then you can finish your answer.

BY MR. SPLITEK:

Q. My question is about column AA, event category.

A. Okay.

Q. Do you see how it says "web" and it never says "file"?

A. I do.

Q. My only question is: Do you make

Page 165

anything of that fact?

A. No.

Q. Okay. In column AI, the event provider column, do you see how in rows 31 through 50 it always says "SharePoint" and never says "OneDrive"?

A. Hold on. AI shows SharePoint, yes.

Q. Okay. And it never shows OneDrive, right?

A. It does not show OneDrive.

Q. Do you make anything of that fact?

A. In a vacuum, no.

Q. How about at all?

A. I agree that that column contains the word "SharePoint."

Q. I mean, does that mean anything to you?

MR. YOSHIMURA: Objection.

BY THE WITNESS:

A. Well, in a vacuum, no. One has to consider all of the columns to -- for me to form an opinion as to what that activity has been recorded. So, for example, SharePoint if we go -- let's see if we got the -- yeah, so if we go to column GG.

Page 166

Q. Yes.

A. You see, it's Ecolab, SharePoint, we've got sales portal, products, products, documents. So, yes. So, okay, so it does -- again, this is why -- I'm answering your questions.

So OneDrive correlates to what is known as personal home directories. Each employee is provided with their own OneDrive account. Files can be shared from OneDrive to other employees. That typically is what's known as SharePoint. Other employees think, oh, I have a copy of it in my OneDrive. They don't really have a copy of it in their OneDrive. They have a pointer to it.

As I mentioned earlier, there are other instances where there are, we'll call shared departmental directories, the HR department, the sales department and they are not tied to a single unique employee's OneDrive account.

So we see here in column GG it says Ecolab SharePoint sites products, product documents, Perm-Clean, PC60 membrane, cleaning compound. So that is row 42.

So my opinion, Ms. Grailer accessed this file that, in my opinion, and the evidence is

Page 167

consistent with her exfiltrating this membrane compound that was originally stored in a shared departmental folder in SharePoint, not her personal OneDrive account, not Josh Galliart's OneDrive account, but from a shared -- what I refer to as a shared departmental folder.

Q. Okay. So based on column GG, you are saying that Grailer exfiltrated the files from shared folders in SharePoint, not from her personal OneDrive folders; is that right?

A. Correct. That's what the evidence shows.

Q. Okay. And the fact that the URL's in column GG go to group SharePoint folders would be consistent with the fact that SharePoint is the only value shown in column AI, the event provider column, right?

A. Exactly right.

Q. Okay. In column AJ, the event type column, do you see how it always says "info" and it never says "access"?

A. I see in Exhibit 12, column AJ, it says -- well, it says "info," sometimes "info start access."

Page 168

Q. I want you to focus on rows -- and I probably wasn't clear -- rows 31 through 50, the file previewed events. In the event time column in column AJ, the only value is info; access is never a value, correct?

A. Correct.

Q. Does that mean anything to you?

A. I don't know what that field means.

Q. Okay. I want you to go to page 2, column DF.

A. Okay.

Q. There is an alphanumeric code that appears in rows 31 through 50 of column BF, correct?

A. Okay.

Q. Do you know what that alphanumeric code refers to?

A. I do not.

Q. Did you try to figure it out?

A. I don't recall if I researched that particular code. As I sit here, I don't know what it refers to.

Q. And do you know if column BF is identifying an application?

Page 169

A. I don't know.

MR. YOSHIMURA: Objection.

BY MR. SPLITEK:

Q. Do you know whether the value in rows 31 through 50 of column BF of Exhibit 12 identifies a Microsoft application called People Predictions?

MR. YOSHIMURA: Objection; asked and answered.

BY THE WITNESS:

A. I don't know what those codes in column BF refer to.

Q. Did you do any analysis to determine whether a Microsoft application called People Predictions could have caused the log entries that we see in rows 31 through 50 of Exhibit 12?

A. I've never heard --

MR. YOSHIMURA: Objection.

BY THE WITNESS:

A. I've actually never heard of an application called People Prediction.

Q. Did you do any analysis to determine whether any application could have caused the log entries that we see in rows 31 through 50 of

Page 170

Exhibit 12?

MR. YOSHIMURA: Objection; asked and answered.

BY THE WITNESS:

A. It is my opinion that Jessica Grailer used an undisclosed device to access those files and exfiltrate them on that date.

Q. But that wasn't quite my question.

My question was: Did you do any analysis to determine whether any application could have caused the log entries that we see in rows 31 through 50 of Exhibit 12?

MR. YOSHIMURA: Objection. I think he answered that question and every other question you've asked about those specific cells multiple times now.

BY THE WITNESS:

A. It's my opinion that -- and the evidence is consistent with Jessica Grailer having logged in under her -- these columns are not visible in your Exhibit 11, but we can show -- the columns show, like, the user account is Jessica Grailer.

So it's Jessica Grailer logging in

Page 171

using an undisclosed device to exfiltrate those files, in my opinion.

Q. And my question was just a yes-or-no question about whether you performed any kind of analysis.

How about this: If you performed any analysis to determine whether any application could have caused the log entries shown in rows 31 through 50 of Exhibit 12 now is your time to tell me.

MR. YOSHIMURA: Objection.

BY THE WITNESS:

A. I didn't perform analysis of what -- I analyzed this document. I came to the conclusion, my expert opinion, that a person I believe to be Jessica Grailer logged into her Ecolab account using an undisclosed device and exfiltrated these files.

Q. Is that your whole answer?

A. That is my answer.

Q. All right. Page 2, column DM. Managed device.

A. Yes.

Q. As you pointed out before, rows 31

Page 172

through 50 in Exhibit 12, that value says "false."

What do you make of that?

A. It says it's false.

Q. I know, but what does that mean to you?

A. I'm not sure. But I'm just noting it says "false."

Q. All right. Page 2, collum FV, the source is organization column.

A. Page 2, FV?

Q. Yep. Rows 31 through 50.

A. Hold on. FV. Yes, I see that.

Q. The value is always, "Microsoft Corps MSN As Block?"

A. Uh-huh.

Q. What do you make of that?

A. So I looked at the source IP that's -- well, the column is cut off. It's after FX. It starts 2603.1036. And my recollection is that IP address is owned by Microsoft. So it correlates to their Office 365/s or service.

Q. Okay. And how could Grailer have accessed or previewed the files that are identified in rows 31 through 50 of Exhibit 12 from a Microsoft corporation IP address?

Page 173

A. That's a good question. So some of the entries in here we see the IP addresses resolve to Charter Communications, which, in my opinion, is her home personal Internet account. Some of the IP addresses I looked up, they relate to the Verizon business, the Zscaler. Other IP addresses relate to Microsoft Office 365.

So the report doesn't -- for example, if Ms. Grailer had accessed it -- had accessed and performed this activity from a starting IP address, let's say her home IP address, and then that got forwarded to the Microsoft Office 365 instance, and then the Microsoft instance is what the IP address was recorded, that's any explanation.

Q. And on what basis are you saying that?

A. My basis?

Q. Yes.

A. Well, the IP address resolves to Microsoft Office 365.

Q. But I guess what is -- so you're saying that Grailer was able to access files on January 15th, 2023, without leaving any trace of the IP address she was doing that from?

Page 174

MR. YOSHIMURA: Objection.

BY THE WITNESS:

A. No. No. What I'm say is that the audit log here recorded entries of -- that says source IP address that resolved to Microsoft Office 365.

Q. I can see that. But why -- in other entries, the IP address was her home IP address, right?

A. That's exactly right.

Q. And then in other entries I thought you told me it was the hotspot she received from work, right?

A. Verizon, yes.

Q. What is your explanation for why on January 15th the IP address is a Microsoft corporation IP address in Des Moines, Iowa?

A. I don't know.

Q. Okay. Let's look at column GG on -- so page 3 of Exhibit 12. Still focusing on rows 31 through 50.

A. Okay.

Q. So column GG gives file paths and at the end of the file paths, the file names, right?

Page 175

A. It does.

Q. Okay. So the logs you reviewed do not show any events where any of those files were deleted, right?

A. No. And to answer further, because I'm an independent expert, my recollection is that I actually looked for these files on her laptop to see which ones we still had. Because from my experience, and the other Ecolab cases and other cases I found, it's not uncommon for employees to not only exfiltrate files, but to take steps to delete their former employer's only copies.

So my recollection is that some of these files I could recover from her laptop but other files I couldn't.

Q. But are you opining that she deleted the files that you couldn't find?

A. My recollection of my analysis is that some of the files -- I didn't include it in my report. At that point when I was writing my report, I didn't think it was relevant. But some of the files I was able to recover and some of the files I was not.

As I sit here, I don't have that

Page 176

analysis in front of me. But I do recall running that analysis.

Q. Let's go back to my original question, though, which is whether you could recover them or not, the log does not record any instances of Grailer deleting any of the files identified in rows 31 through 50 column GG of Exhibit 12, right?

A. It does not.

Q. All right. And when you said you looked for those files, did you look for them at the SharePoint URLs that are listed in rows 31 through 50 column GG of Exhibit 12?

A. I recall looking for them on her laptop which also has, obviously, synchronization of her OneDrive account. So I did not -- I was not provided with original copy of the SharePoint shared folders. I was not provided with copies of those and I did not look and analyze the actual SharePoint folders because I was not provided with copies of them.

Q. Okay.

A. But my analysis was looking at her laptop to synchronize with her OneDrive account.

Q. And I understand because you didn't

Page 177

have the information, you did not look for the files at the file paths that are identified in column GG, rows 31 through 50 of Exhibit 12, right?

A. I did not.

Q. Okay.

MR. YOSHIMURA: We've been on the record for quite a while here. Are we going to be able to take a break pretty soon?

MR. SPLITEK: We can take a break whenever. But I'm less than -- I'm five minutes maybe from a more natural breaking point.

MR. YOSHIMURA: Let's get to that breaking point then.

MR. SPLITEK: All right.

BY MR. SPLITEK:

Q. Still looking at column GG, rows 31 through 50 of Exhibit 12. So the URLs in those columns and rows, they go to a number of different folders and sub folders in SharePoint, right?

A. They do.

Q. Did you do any analysis to determine whether a user could access 20 specific files in

Page 178

all those different folders and subfolders within only a couple seconds?

A. No.

Q. And I just want to make sure that we're clear. If we turn to the last page of Exhibit 12, rows 31 through 50 of Exhibit 12 looking at columns GP and GT.

A. Yes.

Q. What do you make of the fact that columns GP and GT are empty in rows 31 through 50 of Exhibit 12?

A. I don't know why they're empty.

Q. All right.

MR. SPLITEK: As promised, I'm ready for my break.

THE VIDEOGRAPHER: The time is 1:09 p.m. We are going off the record.

(Whereupon, a break was taken, after which the following proceedings were had:)

THE VIDEOGRAPHER: The time is 1:59 p.m. We are back on the record.

MR. SPLITEK: Before we begin, let me note on the record, Bruce Pixley has been

Page 179

listening in via Zoom all day and we intend to have him continue to do that for the rest of the deposition.

BY MR. SPLITEK:

Q. I will move on from Exhibit 12, but I want to revisit one thing quick. If you can go back to Exhibit 12.

A. Okay.

Q. And take a look at columns BC and DE in Exhibit 12. That's pages 1 and 2.

Can you tell from the folder tabs shown in columns BC and DE of Exhibit 12 whose calendar events were hard deleted in the hard delete events?

A. I'm not sure I'm understanding your question. So you're talking about referring to Exhibit 12, column BC to being with row 21, it shows calendar Benjamin Irwin.

Q. Yeah. We can focus on -- so rows 24 through 30 --

A. Okay.

Q. -- of Exhibit 12 and column BC it says "Calendar/Irwin Benjamin," right?

A. I see that.

Page 180

Q. And when you drop down to rows 56 through 60 in column BC, it says "Calendar/Patrick M. Severson"?

A. It does.

Q. Okay. And does that tell you anything about whose calendar these events were on?

A. No. I mean, other than -- I don't want to speculate, but my interpretation would be that there was a calendar event with Jessica Grailer and Benjamin Irwin. But if we look at column BD it lists Focus Time, Private Appointment, Pepsi Knoxville Controller Installation Survey, Private Appointment, Focus Time.

So my interpretation of BC and BD is that these are the events that were in Ms. Grailer's calendar with these individuals that were deleted.

Q. And do you know who would have initiated the first deletion of the calendar events?

A. No. But I know that it's -- and it's not included in your Exhibit 12, but one of the columns shows that it was under user account JGrailer@Ecolab.com. So it is my opinion that the

Page 181

activity was performed by Ms. Grailer, not Benjamin Irwin or these other individuals.

Q. And if one person -- hold on.

This is a hard delete event. Is there a distinction between a hard delete and a soft delete?

A. Not that I'm aware of or could opine on that.

Q. All right. Do you know if when one participant in a shared calendar invitation deletes that calendar invitation it deletes in both user accounts?

A. I don't know. I have not investigated that.

MR. SPLITEK: All right. Let's take a look at Exhibit 13.

(Deposition Exhibit No. 13 was introduced to the witness.)

BY THE WITNESS:

A. Okay.

Q. Are you familiar with the materials in Exhibit 13 that Microsoft makes available online?

A. I'm not familiar with this particular document, but I regularly refer to Microsoft's

Page 182

website for explanations of information.

Q. Do you know if the materials marked as Exhibit 13 can be helpful to interpret any of the log terminology we've just been looking at in Exhibit 12 --

MR. YOSHIMURA: Objection.

BY MR. SPLITEK:

Q. -- and the earlier exhibits?

A. I don't recall looking at this particular Microsoft guide, for lack of a better term, relating to audit log activities.

MR. SPLITEK: All right. Exhibit 14 I will hand you.

(Deposition Exhibit No. 14 was introduced to the witness.)

BY MR. SPLITEK:

Q. Are you familiar with the materials in Exhibit 14 that Microsoft makes available online?

A. I am not.

Q. Do you know if the materials marked as Exhibit 14 can be helpful to understand the hard delete events that we reviewed in Exhibit 12?

MR. YOSHIMURA: Objection.

Page 183

BY THE WITNESS:

A. I have not read this particular guide, so I can't opine on it.

MR. SPLITEK: All right. I'll hand you Exhibit 15.

(Deposition Exhibit No. 15 was introduced to the witness.)

BY MR. SPLITEK:

Q. Are you familiar with the materials in Exhibit 15 that Microsoft makes available online?

A. Again, I regularly refer to Microsoft's guides online regarding what Microsoft states; for example, what it means by first-stage recycle bin and second-stage recycle bin.

This particular Exhibit 16 I don't have any recollection of ever reading.

BY MR. SPLITEK:

Q. Exhibit 15 you said you don't have a recollection of reading?

A. Not this particular website.

MR. SPLITEK: I'm handing you Exhibit 16.

Page 184

(Deposition Exhibit No. 16 was introduced to the witness.)

BY MR. SPLITEK:

Q. Are you familiar with the company called Elastic that makes the materials shown in Exhibit 16 available online?

A. I am.

Q. And do you know whether Elastic software was involved in producing the large spreadsheet log that we marked as Exhibit 10?

A. I am.

Q. Are you familiar with the materials that I've marked as Exhibit 16 here that Elastic makes available?

A. As I'm reading Exhibit 16, I have not read this particular report or documentation from Elastic.

Q. And do you know whether or not the materials I've marked as Exhibit 16 can be helpful in understanding the event dot category field in the log that we marked as Exhibit 10?

MR. YOSHIMURA: Objection.

BY THE WITNESS:

A. I have not read through this Elastic

Page 185

information in Exhibit 16 so I can't opine on it.

MR. SPLITEK: I'll hand you Exhibit 17.

(Deposition Exhibit No. 17 was introduced to the witness.)

BY MR. SPLITEK:

Q. Are you familiar with the materials marked as Exhibit 17 that Elastic makes available online?

A. I have not read this particular document that is -- I can see from the bottom it was pulled directly from Elastic's website.

Q. Okay. Am I right then that you're not able to opine on whether the material that's marked as Exhibit 17 can be helpful to understand the event dot type field in the log we marked as Exhibit 10?

A. I have not read any of the content in Exhibit 17 prior to today.

Q. And in your report and today during your deposition you've talked about Grailer using an undisclosed computer, right?

A. Yes.

Q. All right. Was that undisclosed computer, as you call it, approved by Ecolab as a

Page 186

device to access its systems?
A. In my opinion, it must have been in the past.
Q. Did you ask Ecolab for a list of all approved devices that accessed its systems on or around January 15th, 2023?
A. I did.
Q. Did you receive that list?
A. As of the date I asked for it, which would have been in February, my recollection is that they had not -- I ran into ground and I don't believe they had any record of which device -- they could provide to me a record of which devices had been approved in the past and which ones hadn't.
Q. Did you ask for a list of all devices that accessed Ecolab's system on or around January 15th, 2023?
A. Yes.
Q. Did you receive that list?
A. I was told -- excuse me. I was told as of the date of my involvement that the sum total of information that I could be provided with from Ecolab systems was encompassed by the Digital

Page 187

Guardian report and the OneDrive audit log and her former work laptop and two former work phones.
Q. And at that time you say the audit log was the smaller one that we marked as Exhibit 9, right?
A. It was.
Q. And who told you that?
A. Jennifer Semmler.
Q. And did Jennifer Semmler say that the other information you asked for didn't exist?
A. I had asked Jack Anderson of Ecolab IT if he had any more information related to approved devices.
Q. And what did Jack Anderson tell you?
A. They didn't have a record of that.
Q. But I also asked about did you -- if you sought a list of all devices that accessed Ecolab's system on or around January 15, 2023. Did you seek that?
A. On or around January 15th?
Q. Yes.
A. So as part of my analysis I analyzed Jessica Grailer's former Ecolab work laptop to see if I could find any reference to another computing

Page 188

device. I did not find any on her work laptop.
I analyzed the Digital Guardian report to see if I could find any reference to any other -- what I'm referring to the undisclosed device. I didn't find any reference in the Digital Guardian report.
Q. I understand all of that.
I'm asking, did you ask Ecolab for a list of devices that accessed its system at any time?
A. Yes.
Q. Not whether they were approved or unapproved, just a list of devices that accessed its systems, you asked for that?
A. Yes.
Q. And what were you told?
MR. YOSHIMURA: Objection.
BY THE WITNESS:
A. I was told as of the time I made the inquiry that that information -- that all the information that was available was what I described; the Digital Guardian report, the user audit log --
Q. Okay.

Page 189

A. -- and the devices I was provided with.
Q. All right. In your report you talk about Grailer emptying her computer's recycle bin on January 8th, 2023, right?
A. I do.
Q. All right. Do you know what happened to the files in Grailer's recycle bin after she emptied it?
A. Do I know what happened to the files? Well, my forensic tool, OSForensics, was able to carve, C-A-R-V-E, carve and recover some of the deleted files. And even though the recycle bin, as of the date that the laptop was provided to me, the recycle bin had been emptied by, I believe, Ms. Grailer.
But my forensic tool was able to carve and recover some deleted files from -- that had been stored in the recycle bin.
Q. Let me ask you a better question.
You mentioned the second-stage recycle bin earlier, right?
A. Yes.
Q. Do you know whether the files that Grailer emptied from her recycle bin on January

Page 190

8th, 2023, then moved to the second-stage recycle bin?

A. Well, respectfully you're conflating two items. So first-stage recycle bin and second-stage recycle bin is Microsoft terminology related to deletion of files that exist in a OneDrive account online.

What I was referring to in my report being able to carve and recover files from the Jessica Grailer laptop, I was referring to my ability to carve and recover those files from the local laptop hard drive. So that is completely unrelated to first-stage recycle bin and second-stage recycle bin on OneDrive. That's data stored in OneDrive versus data stored on the physical laptop.

Q. Okay. So to be clear then, when you talk about Grailer emptying the recycle bin on her laptop, you are not opining that any files stored on OneDrive were thereby deleted, correct?

A. Correct.

Q. Do you know whether or not when Grailer put files in her recycle bin on her desktop copies of those files then went into a recycle bin in

Page 191

Grailer's OneDrive account?

A. So I believe what you're asking me -- you may not be asking this question but maybe the question you should be asking is, it is possible -- so on the local laptop we'll see there is a C, which is the local drive, user name then OneDrive, and then folders and files. So that's what we'll call the OneDrive synchronization folder. So those files exist both on the local laptop because they're synchronized down to the laptop and they exist also in Microsoft's OneDrive. So they actually exist in two locations.

And the question I think you're asking is if one were to delete a file from, let's say, the local files stored within that OneDrive path -- we see that in some of the files in my reports from the local laptop -- would that also delete the version that's stored online. And that's a very specific question.

I think it can be. But I would -- I'd have to analyze the computer and test that to see how Ecolab set up their synchronization. It is possible -- I know from experience it is possible

Page 192

to set it up such that if a file is deleted from the local laptop hard drive within the OneDrive folder, the next time it synchronizes online, it will delete it from the online folder because -- well, the user -- most end users don't realize that.

When they're seeing a OneDrive folder, they think it's all online. But it's really the local version.

So is that what you're asking me is if I deleted it from the OneDrive -- a document from the OneDrive folder that's stored on the local hard drive, would it cause the online copy in Microsoft's Azure system to be deleted as well?

Q. No. But that was still helpful so thank you.

You referred to some settings. Those are settings that Ecolab would have controlled, synchronization settings?

A. It is either Ecolab or -- it's Microsoft. It's how they set up synchronization.

Q. And you don't know what the synchronization settings were?

A. Not as I sit here. I believe they can

Page 193

be tweaked so they can make it such that even if a file is deleted locally, it still exists online. Or if it is deleted from the local OneDrive folder, the next time it syncs it is deleted from the online OneDrive but that's a Microsoft setting, so ...

I don't believe I opined on anything related to that in -- when I refer to this file deletion in the recycle bin I was specifically -- I apologize if this was not clear in my report -- deletion of files from the local laptop hard drive and then the fact that when I received the laptop, the local laptop recycle bin was empty.

Q. Thank you. That is helpful.

The question I was asking earlier though was -- I'll try to rephrase it.

When Grailer would put local files from her laptop into her local recycle bin, do you know whether or not there was also a recycle bin on OneDrive that would be synchronized with her local recycle bin?

A. I don't believe so. My understanding of the way OneDrive synchronization works is Microsoft will set up a OneDrive folder on the

Page 194

local hard drive that will contain -- you know, synchronize so that employees can access these OneDrive folders when they're offline.

And I believe it is possible to extend that. I believe now Microsoft has expanded that so that not only the OneDrive folder is synchronized up and down, but also the desktop folder and maybe my documents. But that's Microsoft doing that. So it is -- yeah.

MR. SPLITEK: I'm going to hand you Exhibit 18.

(Deposition Exhibit No. 18 was introduced to the witness.)

BY MR. SPLITEK:

Q. Are you familiar with the materials in Exhibit 18 that Microsoft makes available online?

A. I have not read this particular entry from Microsoft.

Q. Okay. Then am I right then that you don't know whether or not Exhibit 18 contains information relating to how the second-stage recycle bin works?

MR. YOSHIMURA: Objection.

Page 195

BY THE WITNESS:

A. Well, I am aware of how Microsoft's second-stage recycle bin works, according to Microsoft.

Q. How does it work?

A. According to Microsoft's website themselves and Microsoft, when a file is placed on -- it's moved from the first-stage recycle bin to the second-stage recycle bin, it can no longer be recovered. It's the equivalent of -- so the first-stage recycle bin is the trash receptacle next to my desk, and then the second-stage recycle bin would be the dumpster behind the dumpster outside of the building.

Q. And are you saying that once it's in the second-stage recycle bin, the file can never be recovered again?

A. That's what Microsoft says.

Q. By anybody, including the system administrator?

A. According to Microsoft, it can no longer be recovered.

Q. Okay. Once it's in -- as soon as it enters the second-stage recycle bin, it's gone

Page 196

forever to everybody, right?

A. According to Microsoft.

MR. SPLITEK: I'm going to mark -- I'm going to hand you Exhibit 19.

(Deposition Exhibit No. 19 was introduced to the witness.)

BY MR. SPLITEK:

Q. Exhibit 19, is this a copy of Exhibit G to your report?

A. It could be. Now I'm really ruing the fact that I didn't bring my reading glasses.

Q. I also was not happy with your small print Exhibit G.

A. What I'm going to do is take a picture of it.

Q. That's okay with me. I'm fine with that.

MR. YOSHIMURA: I think this is the same as the Exhibit G that's in the packet that you provided earlier that was printed.

MR. SPLITEK: Is that bigger?

MR. YOSHIMURA: It is not printed.

MR. SPLITEK: I'm fine with him looking at that. I'm also fine if he wants to use

Page 197

his phone to magnify. I don't have any objection. That's fine.

THE WITNESS: I can't read this.

BY MR. SPLITEK:

Q. Let's try to talk generally about Exhibit G and if there is another -- there is also Exhibit G within --

MR. YOSHIMURA: Exhibit 3.

MR. SPLITEK: In Deposition Exhibit 3, you can look at that one too. I'm just trying to pull it out so there is one clean record of it.

MR. YOSHIMURA: Understood. Here, I'll trade you.

MR. SPLITEK: We could not have more copies of Exhibit G.

THE WITNESS: Okay. I'm recalling.

BY MR. SPLITEK:

Q. We agree we are looking at Exhibit G to your report?

A. We are.

Q. And that's what I've also marked as Exhibit 19, right?

A. It is.

Page 198

Q. Okay. So in your report you say that Grailer deleted all of the files listed in your Exhibit G on January 8th, 2023, right?

A. I believe so.

Q. So I want to look at the first ten rows --

A. Okay.

Q. -- of Exhibit G.

A. Okay.

Q. If you look at the file path which is page 1 of Exhibit G --

A. Okay.

Q. -- in the file path do you see, again, that INetCache/content.Outlook folder?

A. I do.

Q. Did you testify earlier that that's a system folder that typically a user isn't managing?

A. Yes.

Q. Okay. So when files were deleted from the INetCache folder, might that have been the system automatically deleting files that were cached?

A. I don't recall finding evidence of

Page 199

automatic system deletion versus Window's system deleting files.

Q. And tell me again, what do you believe the function is of the INetCache folder in relation to the files that are shown in those first rows in your Exhibit G?

A. My understanding is it is a system folder that records and stores evidence of human interaction and temporary files. So, for example, someone opens up an e-mail attachment or opens up an Internet using their Internet browser, Windows Explorer will create a temporary copy, and that's resulting in these.

Q. So these were temporary copies of files shown in the first ten rows of Exhibit G?

A. It could be.

Q. Did you check to see whether these temporary copies of files related to files connected to Grailer's work e-mail activity on January 8th, 2023?

A. I don't understand the question.

Q. Do you know whether or not the files listed in the first ten rows of your Exhibit G are -- were just temporary copies of files that were

Page 200

attached to e-mails that Grailer sent or received on January 8th, 2023?

A. So it is my opinion and the evidence is consistent with these files being deleted as a direct result of actions Jessica Grailer took.

Q. That's not my question.

My question is: Do you know whether or not the files listed in the first ten rows of Exhibit G were temporary copies of files that were attached to e-mails that Grailer sent or received on January 8th, 2023?

A. It is my opinion the evidence is consistent with the fact that Jessica Grailer deleted these files and moved them to the recycle bin and then emptied her recycle bin.

Q. Well, we're going to try this a different way here.

This is your opportunity to tell me if you have a reason to believe that the files listed in the first ten rows of Exhibit G were not temporary copies of files that were attached to e-mails that Grailer sent or received on January 8th, 2023.

MR. YOSHIMURA: Objection to form.

Page 201

BY THE WITNESS:

A. So, in my opinion, the files listed in the first ten rows were deleted and placed in the recycle bin as a result of Jessica Grailer deleting those files.

Q. Okay. And you didn't really address whether they were temporary copies of files that were attached to e-mails that Grailer sent or received on January 8th, 2023, that's okay with me.

Do you have anything --

A. I have no evidence that Windows deletes -- would have deleted these files on its own. I found no evidence of that.

Q. Did you ever look to check and see if the files listed in the first ten rows of your Exhibit G were, in fact, attached to e-mails that Grailer sent or received on January 8th, 2023?

A. No.

Q. Then there is a lot of files in your Exhibit G that begin with a "$R" prefix.

A. Yes.

Q. And I want to, for the court reporter, this is a dollar sign and then a capital R to make

Page 202

sure that is clear.

So they have long file names but the prefix always begins with $R, right?

A. It does.

Q. So when a user deletes a file, the file is moved from the original folder to the user's recycle bin, right?

A. That is correct.

Q. And when the file is moved to the recycle bin, it's given a new file name that starts with a $R prefix, right?

A. That's exactly right.

Q. So the $R prefix files in your Exhibit G are files that were sitting in Grailer's recycle bin when she emptied it, right?

A. Correct.

Q. Did you check to see how long those files had been accumulating in her recycle bin?

A. Let me see if I can I understand that question. If you're asking me if I analyzed when each file was deleted --

Q. That's exactly what I'm asking you.

A. I don't recall doing that. What I recall doing and describing in my report is that I

Page 203

used the OSForensics software, the industry standard tool that I'm certified in, to carve and recover files from the laptop.

I was able to carve and recover the files that I described in my report and, again, importantly in my opinion, the recycle bin as the laptop that was provided to me, it was emptied by a person I believe to be Jessica Grailer.

Q. Did you do any analysis to determine how many of the $R prefix files in your Exhibit G were already in the recycle bin before January 8th, 2023?

A. I don't recall performing a file-by-file analysis to determine what date each of the files was placed in the recycle bin. My recollection is that the last modified date of -- from the master file table entry is the date -- equals a date that a file was placed in the recycle bin. But I didn't feel I needed to perform that analysis.

I just know that what I identified and described in my report can be independently verified and replicated by a qualified peer.

Q. And you can look in the USN change

Page 204

journal to identify specific files that Grailer put in her recycle bin on January 8th, 2023, right?

A. I have not done that in this case.

Q. I asked if you could do it.

A. Possibly. I have not done it, so ...

Q. Okay. But I guess then bottom line, you don't know how many of the $R prefix files in your Exhibit G were already in Grailer's recycle bin before January 8th, 2023, right?

A. I don't know. I didn't perform that analysis.

Q. Then there's a lot of files in your Exhibit G that begin with a $I prefix, right?

I'll make sure for the court reporter it's clear, it's dollar sign and then the capital I.

So I want to make sure we understand what a $I prefix file is. I wish these had names that were more pleasant to say.

A. So when a user of Windows computer places a file in the recycle bin, you're correct that Windows renames that deleted file with this $R and whatever, A, B, C, D, E.

Page 205

At the same time the Microsoft Windows operating system will create a paired file that's $I, the same string, A, B, C, D whatever. The $I file is a system artifact that, amongst other information, contains the original path from which the file was -- or originally existed on the laptop before it was deleted and the file name.

So for example, the $I might show C:user/JGrailer/desktop/Nalcodocuments and whatever report dot PDF.

So analysis of the $I file can reveal not only the name of -- the original name of the file that's been changed to $R but also the location from which the file was moved to -- you know, before it was moved to the recycle bin.

Q. All right. And just for an example here, if we can somehow all see it, on page 1 of your Exhibit G, we went through this first ten rows where the file path goes to the INetCache folder. But just look at the next two rows as an example.

A. Okay.

Q. The first row is an $R file, and then the rest of the file name is 047B1E, right?

Page 206

A. Yes.

Q. Then the next row down is a $I file, and the rest of the file name is identical, again, 047B1E, right?

A. It is.

Q. Okay. So the $I file, did you refer to that as a system artifact?

A. It's a system artifact that has the original -- so if a user -- if you ever go in your recycle bin and selected a file that you deleted and say I want to restore this file, well, Windows knows where to restore it to based upon that $I file. So when you restore it, it will go back to the original location within your desktop or your downloads. It doesn't just go to a random location. It goes to the location from which it was originated from, and that's the $I.

Q. Okay. And $I prefix files, are they sometimes called recycle bin information files?

A. I have not heard them referred to that, but that sounds accurate.

Q. Sounds better than $I.

A. Yes.

Q. Okay. Let's stick with $I, though,

Page 207

since you hadn't heard of the other one.

So Windows automatically creates the $I prefix files in the recycle bin, right?

A. Yes. And in some cases -- I don't know if it is the case here because I have not looked at all of these and I don't have my glasses on, but in some cases, my forensic tools have only been able to recover the $I file, not the $R, the actual deleted file.

In those cases -- again, I don't know if it's the case here -- I've been able to opine that a file did exist on the computer based upon -- even though it's no longer accessible, it was probably overwritten after a file is deleted, so sometimes I get the $I and the $R file, then I can restore the actual $R which is the actual file.

Sometimes I'm only able to restore the $I file, but then I can opine on what file was deleted and where it existed before it was moved to the recycle bin.

Q. And typically the user wouldn't see the $I prefix files, right?

A. I don't think they're seeing $I or $R.

Page 208

Those are -- only our forensic tools are seeing those.

Q. Okay. Those are not visible to a user like Grailer?

A. No.

Q. When the recycle bin is emptied, the $I prefix files can be emptied -- could be deleted, right?

A. Yes. But, again, so our forensic tools can carve and recover files that have not been overwritten through continued usage and are still available to be recovered.

And so in this case, the OSForensics tool, one of its features is that it carves and recovers deleted files. So I performed that analysis, which is standard on all of my cases.

Q. But when a user opens the recycle bin, they don't see the $I prefix files in there?

A. No. It's a hidden system file.

Q. Okay. And they didn't put the $I prefix files in the recycle bin either, right?

A. No. They didn't put them in there. The $I files are a system file that's created by the Windows operating system when a file is moved

Page 209

to the recycle bin.

Q. And I guess the question then is why, in your report, are you accusing Grailer of deleting these system files that a user generally wouldn't even know about?

MR. YOSHIMURA: Objection.

BY THE WITNESS:

A. Well, these files were all carved and recovered by my forensic tool, and so these are -- so they are files, the $I files.

I understand what distinction you're making is that it's a system file that Ms. Grailer would not have been able to see. But it's still a -- the point I was making is it's still a file that my forensic tool was able to carve and recover.

And as I said, I don't know if it's the case here, if we only see a $I and not a paired $R, then it will be the case; and oftentimes I'm only able to carve and recover the $I file, which informs me that there was an actual deleted file that got overwritten and was not able to be recovered. I've had that on many cases.

Q. Let me make sure I'm clear then.

Page 210

In your Exhibit G, were you able to recover the $I prefix files listed in Exhibit G?

A. Yes.

Q. So those were not permanently deleted; is that right?

A. That's exactly right. All the files listed were able to be carved and recovered by my forensic tool.

Q. Okay. Are there any files listed in your Exhibit G that you were not able to recover?

A. Again, I don't recall seeing any files where only one can see the $I version and not the paired $I A, B, C, D, E. There should be a paired $R A, B, C, D, E; the $R A, B, C, D, E being the actual PDF file or Word file.

But as I'm sitting here, it is possible. So if you see one of these that's only the $I and there's no paired $R, then, in my opinion, that would be an example of my forensic tool being able to recover the system file but the actual file was overwritten.

But as I sit here, I don't recall seeing anything like that. I didn't look.

Q. Okay. So to the best of your

Page 211

knowledge, none of the files listed in your Exhibit G were permanently deleted?

A. No, because -- yeah, because what I describe as permanent deletion is deleted beyond recovery, meaning overwritten.

Again, sometimes I'm able to recover the $I designation that can show me that a file did exist even though the file wasn't able to be recovered, but I can opine with 100 percent that a file did exist on a computer but it was no longer able to be recovered.

Q. But to the best of your knowledge, none of the files listed in your Exhibit G was deleted beyond recovery?

A. Again, if one of these in here we only see the $I but not the paired $R file, then I would describe those files as permanently gone.

But as I sit here, I don't recall doing that analysis to see if there was only a $I and not -- which is the system file saying there was a file that existed at this path on my documents. So I don't know. It is too small for me to see if there's -- the pairs are there or not.

Q. All right.

Page 212

A. I didn't think it was relevant.

Q. So when Grailer connected and disconnected her USB thumb drive to and from her laptop, that caused multiple timestamps to update in Windows; am I right?

A. Yes.

Q. Not just one timestamp but multiple timestamps in different places in Windows would update, right?

A. Right. The act of connecting a USB drive to a Windows operating system will create timestamps in a variety of locations on a Windows laptop.

Q. And one of those locations is in what's called the mount -- try again -- one of those locations is in what's called the MountPoints2 sub key of the Windows registry; is that right?

A. It could be. I know it's in the USBSTOR file. It's in -- it's recorded in -- Windows records activity in a lot of places.

Q. Yeah. And let me pause real quick to tell the court reporter, if it's okay with you two. MountPoints2, it's capital M-O-U-N-T, capital P-O-I-N-T-S and then the number 2.

Page 213

Do you think I got that right?

A. I'm not familiar with that particular one. But I know event logs, Windows event logs that end in dot EVTX can and will record activity of USB drive interactions, the USBSTOR file. There is various locations.

I'm blanking on the other ones. Windows captures this information in a variety of locations.

Q. Okay. Let's just focus on when she connects her USB thumb drive to the computer. So I think you said you're not sure whether or not a timestamp is updated in the MountPoints2 sub key of the registry, right?

A. I would have to test that. I don't know that, as I'm sitting here.

Q. Okay. But there is at least one timestamp and maybe more in the USBSTOR sub key that updates; is that right?

A. I believe so.

Q. Let me pause to try to spell USBSTOR -- Mr. Lieb, do you want to try it?

A. It's U-S-B-S-T-O-R, no E at the end.

Q. All right. And all in caps?

Page 214

A. All caps.
Q. U-S-B-S-T-O-R.
A. And various event logs.
Q. Yes. When Grailer would connect her USB thumb drive to the laptop, it would create an entry in the Windows event logs, right?
A. That's why it's very difficult for a layperson to try and cover their tracks on a Windows computer because most people aren't aware that evidence of activity appears and is recorded in 20 different locations.
Q. Because there are event logs that show every time you connect and disconnect a USB device?
A. Plug and play logs, registry, yes.
Q. Yes. Okay.
A. A variety of places.
Q. And then there's also -- we mentioned the USBSTOR sub key. There's also something called a USB sub key, right?
A. Could be. I'm not familiar with that one. You could be right.
Q. Okay. And I want to -- --
A. Are we done with this exhibit?

Page 215

Q. Yes, we are. Don't throw it away but we're re done with it for now.

And I'll tell you how I'm spelling things. So USBSTOR, again is, all caps U-S-B-S-T-O-R and then USB is just all caps U-S-B.

So we covered already that there is something called the USBSTOR sub key in the registry, right? We agree with that?
A. Yes.
Q. Do you know whether there is also something called USB sub key in the registry?
A. I'm not familiar with that reference, but when I do a USB device analysis I do it regularly on every case.

So it's in the Microsoft -- sorry, Magnet Forensics Axiom tool, which I used in this case, it just has a sub folder that says devices, connected devices and it will list USB drives.

It also has devices in another location where it will have references to USB device interactivity. So it actually -- I don't know why Axiom records it in two different locations, like devices and also USB devices. But it will ...
Q. And this information is also reported

Page 216

out by OSForensics, right?
A. It is.
Q. And let me pause since we're on the topic of terminology to make sure we have a couple things clear.

You used Axiom software to extract information from the image of Grailer's laptop, right?
A. I did.
Q. And the developer of Axiom is Magnet Forensics, right?
A. Correct.
Q. So when you extracted information using Axiom from the image of Grailer's laptop, you then got -- would you call it a case or a database? What is your preferred term?
A. It's a case. I was asked to produce a copy of that and I did.
Q. That's what Mr. Pixley calls it too; a case.
A. Yeah, Magnet Forensics refers to it as a case file.
Q. All right. Yeah, a case or a case file. Can we call it a case right now?

Page 217

A. Yes.
Q. All right. So you used Axiom to extract image -- you used Axiom to extract information from the image of Grailer's laptop?
A. I did.
Q. And then you got an Axiom case with the extracted information?
A. That's correct.
Q. In a much more readable format than it existed in the image of her laptop, right?
A. That's exactly right.
Q. All right. And then does OSForensics serve a similar purpose?
A. Yes, it does.
Q. And OSForensics, by the way, is capital, O, capital, S, capital, F Forensics, right?
A. That's right.
Q. Okay. So you also used OSForensics, is it fair to say, it's a competing software tool?
A. It is a competing software.
Q. Okay. You also used OSForensics to extract information from the image of Grailer's laptop, right?

Page 218

A. I did.

Q. And then you got -- would that be called an OSForensics case?

A. There is a case folder, yes.

Q. All right. So can we refer to those as your Axiom case and your OSForensics case?

A. Yes, we can.

Q. And I think we got the OS -- no, we got the Axiom case but not the OSForensics case, if I'm not mistaken.

A. Correct.

Q. All right. And both Axiom and OSForensics extract and report timestamp information from multiple sources in Windows, right?

A. The reason I personally used two tools on the same evidence is that almost every single case, the two different tools, they're highly respected, they're used by US law enforcement and US military, will extract the same and report on the same evidence and in one tool it will extract and report on evidence -- or Axiom will extract and identify evidence that OSForensics does not, and vice versa. OSForensics will extract.

Page 219

So my best practice is not just run one tool. I like to -- I always create two different cases and the two different tools, see where the overlap is, and then look to see what is one tool reporting that the other is not, and then dig into that; go, okay, Axiom identified this information, I'm not showing up in the OSForensics. I'm going to look into OSForensics and see why it's not there. Sometimes I'll reach out to Passmark or -- who's the owner or manufacturer of OSForensics, and say, hey, you missed this. They'll update it for the next -- and vice versa.

Yeah, I can't explain it why. But some experts I've encountered say, oh, no, I can only use one tool. And I can prove that's not a good idea.

Q. And I want to go back to the USBSTOR sub key which you're familiar with. Let's just assume for a moment that there is also something called a USB sub key. Would you have any idea what the difference between those is?

A. I'm not familiar what the distinction is.

Q. Okay. Each time a USB thumb drive is

Page 220

connected to the computer, it is mounted and assigned a drive letter like drive D; is that right?

MR. YOSHIMURA: Objection.

BY THE WITNESS:

A. It can be. In some instances, so if a drive is purchased, a raw drive is purchased out of the box and it has never been formatted, formatting means creating like -- what is the best way to describe a format?

So literally all storage devices in the Windows context are file cabinets. In the Windows context, all USB storage device and hard drives, they reserve the first part of the first file cabinet for an index like a Dewey Decimal card catalog -- when they used to have card catalog systems.

And so those card catalog systems in the first part of the first cabinet drawer keep track of when files are created and where they're stored in the file cabinets, if a file is deleted.

So if a file is deleted, in quotation marks, what Windows is doing is just going to the card catalog system and then checking a box. That

Page 221

file still exists in the file cabinet so I can delete all the files on a USB drive, and if I just never touched it, I can recover them all.

So I'm not destroying and overwriting those deleted files in quotation marks. I'm just going into the card catalog system and saying, you know, if you need to use that space again for future files, I can do that.

Q. And I think -- if you don't know the answer to these questions, that's fine, but I want to make sure that I have all of the information that I can get on the record here.

I think you did say you are not familiar with the MountPoints2 sub key; is that right?

A. I've been doing the forensic analysis for close to 20 years so I'm -- I know I've encountered locations where all the different locations in a Windows operating system, be it in the registry or other system files where USB data related to USB data can reside.

Q. Okay. Do you know whether or not the MountPoints2 sub key hierarchy in Grailer's laptop contained a sub key for Grailer's USB thumb drive?

Page 222

A. I don't know. I don't know. As I sit here, I can't recall what you're specifically asking for.

Q. And do you know whether when Grailer's thumb drive was inserted into the computer the last written timestamp for that sub key in the MountPoints2 sub key would update?

A. I don't recall.

MR. SPLITEK: Okay. I'm going to hand you Exhibits 20 and 21 as a pair.

(Deposition Exhibit Nos. 20 and 21 were introduced to the witness.)

BY MR. SPLITEK:

Q. And you'll understand why they're paired when you see them. Exhibit 20 is a screenshot taken from your Axiom case and Exhibit 21 is a zoomed-in enlargement of the text in the right-hand column of Exhibit 20.

A. Okay. I see.

Q. All right.

A. Exhibit 21 is actually -- it says "evidence source." It's highlighted in blue. The information that's being described is actually

Page 223

coming from what is known as the NTUSER.DAT file.

Q. Okay. And what does that mean to you?

A. The NTUSER.DAT file is a Windows operating system file that records various aspects of human interaction within a Windows computer.

Q. And if you look under the evidence source -- we're in Exhibit 21 right now -- under the evidence source there is a location. Does that mean anything to you?

A. So software, I believe that -- so there's -- the Windows registry has multiple, what they call or refer to as hives. There's a software hive, there's a system hive, there's a security hive.

So I assume this is referring to the software registry hive.

Q. So there's a timestamp on Exhibit 21.

A. Okay.

Q. Do you have any idea what that timestamp is telling us in Exhibit 21?

A. Well, it says, "last written time, December 20th, 2022, 6:26 a.m."

But let me see what it is deciding is the last written time. It could be referring to

Page 224

the mount -- the file above it that is starting BC602. I'm not actually sure. As I look at this, I'm not sure whether -- what specifically it is saying was last written.

Q. Do you recall ever looking at the timestamp of the evidence referenced in Exhibit 21?

A. As I sit here, no. But I do recall bookmarking. Actually I think the version of the Axiom case I turned over actually had all of my bookmarks and tags in it. So the information that I analyzed and tagged was all in the Axiom case.

Q. Can you go back to Exhibit 8. Keep Exhibit 21 around but go to Exhibit 8. It is your February 2023 declaration.

A. Okay. I've got it.

Q. Page 8 --

A. I've got -- 8 starts with Exhibit C.

Q. Yeah, Exhibit 8, if you keep turning, it's your February 2023 declaration.

A. Okay.

Q. And if you go to page 8 of your February 2023 declaration --

A. Okay.

Page 225

Q. -- and then if you look at footnote 5 on page 8 of your February 2023 declaration --

A. Okay.

Q. -- if compare your footnote 5 there on 8 of your declaration with Exhibit 21, are you, in fact, citing the same evidence in your declaration in February that is now shown in Exhibit 21?

A. It looks like -- so I got paragraph 26, "Forensic analysis of the laptop reveal that Jessica Grailer plugged in the Emtec external USB drive, serial number 789127BD 070B4A71ADB22353 to the laptop on December 20th, 2022, at 6:26 a.m.," and it says 32 seconds, "and unplugging the USB drive on December 20th, 2022 at 4:55 p.m." And I believe that is footnote 5.

Q. It is footnote 5. That's what I want you to be looking at.

A. Okay.

Q. Look at footnote 5.

A. Okay.

Q. And particularly look at the end of footnote 5.

A. Okay.

Q. Software, Microsoft Windows current

Page 226

version explorer MountPoints2, and then the same alphanumeric code that we see --

A. Okay.

Q. -- in Exhibit 21 next to both the word "path" and the word "location," right?

A. I see that.

Q. So in footnote 5 of your February 2023 declaration, you cited the same evidence that is shown here in Exhibit 21, correct?

A. Yes.

Q. When you cited that evidence in your February declaration, what were you -- what proposition were you citing it for?

A. I believe it was in the context of Jessica Grailer's interaction on December 20th with files related to her new position at Chem Tree.

Q. Well, that's not correct because in paragraph 26 of your February 2023 declaration, you are talking about her plugging in her Emtec external Emtec USB drive into the laptop.

A. Okay.

Q. And then you drop a footnote and you cite the evidence that is now shown in Exhibit 21,

Page 227

right?

MR. YOSHIMURA: Objection.

BY THE WITNESS:

A. So I see that on -- I don't have -- I don't have this February declaration memorized. But I also see around that time frame that in the December 20th time frame that she was accessing files from the Emtec drive related to her --

Q. I understand that. But I want you to focus on what this footnote --

A. Yeah, it says MountPoint2, yes.

Q. Yes, the footnote 5.

A. Okay.

Q. And the footnote you have appended it to paragraph 26 of your February declaration --

A. Okay.

Q. -- which is about Grailer plugging in and unplugging the USB drive, correct?

A. Correct.

Q. And then you cite Exhibit 21 which, in fact, gives a December 20th, 2022 timestamp, right?

A. Yes.

Q. So were you siting this evidence shown

Page 228

in Exhibit 21 for a timestamp of when she connected her thumb drive to the computer?

MR. YOSHIMURA: Objection.

BY THE WITNESS:

A. I don't recall.

Q. Okay. Do you know whether or not Grailer could have connected her thumb drive to the computer again after December 20 of 2022 without updating the timestamp that is shown in Exhibit 21?

A. I have not tested that, but my forensic analysis did reveal evidence of Grailer later connecting that same USB -- that Emtec drive to her former work laptop on January 8th.

Q. But we see in Exhibit 21, which comes from your Axiom case, that the timestamps shown in Exhibit 21 did not update after December 20th, 2022, right?

A. So this information is consistent with what I'm sitting here in paragraph 26 and there is evidence that can be independently verified of her --

Q. That's not my question.

What we're seeing in Exhibit 21 is that

Page 229

the timestamp shown in Exhibit 21 did not update again after December 20th, 2022, correct?

MR. YOSHIMURA: Objection, form. And if you can limit crosstalk, Matt, please. Thank you.

BY THE WITNESS:

A. So I stand by what -- on paragraph 26, page 8 of Exhibit 6.

Q. I know he doesn't want crosstalk, but I'm sorry, you're just not answering the question.

We're going to do this again the other way, which is here is -- after I stop talking -- this is your opportunity to tell me if you think that the timestamp shown in Exhibit 21 ever updated again after December 20th, 2022.

MR. YOSHIMURA: Objection; form.

BY THE WITNESS:

A. I could perform that analysis. I don't recall performing that analysis. I do recall performing analysis that showed -- and it could be independently verified by any qualified peer, that this Emtec drive was also connected to the laptop on January 8th.

Q. You said that when Grailer connected

Page 230

and disconnected her thumb drive from her laptop, Windows would create event log entries relating to these connection and disconnection events, right?

A. It could have.

Q. It could have or it did?

A. I don't recall, as I sit her. I don't have the Axiom database from my OSForensics case in front of me.

MR. SPLITEK: Let me hand you a copy of Exhibit 22.

(Deposition Exhibit No. 22 was introduced to the witness.)

BY MR. SPLITEK:

Q. So I will tell you Exhibit 22 are screenshots taken from your Axiom case --

A. Okay.

Q. -- and do you see that what has been brought up here are the Windows event logs for storage device events, right?

A. Yes.

Q. So do you see in Exhibit 22 there are connection and disconnection events for Grailer's USB thumb drive running from March 16th of 2022, through December 20th of 2022?

Page 231

A. I see in Exhibit 22 under Windows event logs storage device events you have something highlighted in blue that says -- well, there is a line above it, says "connected USB disc 2.0 connected." It has a USB vendor. It doesn't record to Emtec.

But I believe -- if I'm looking at it, it's the same serial number. So, in my opinion, it's the Emtec drive. It shows being connected 6:26 a.m. and then later disconnected 4:55 p.m., which is consistent with the language in page 8, paragraph 26 of my February 2023 affidavit.

Q. And when is the -- as shown in Exhibit 22, when is the last Windows event log for Grailer's thumb drive being connected or disconnected?

A. I can't see the entire -- I don't know if it is showing the entire database. Again, if I had the Axiom case database in front of me and the OSForensics case in front of me, I could answer your questions.

Q. Right now let's just focus on reading what is in front of you in Exhibit 22.

So in Exhibit 22, when is the last

Page 232

event log entry that you see for Grailer's thumb drive?

MR. YOSHIMURA: Objection.

BY THE WITNESS:

A. For the Emtec?

Q. That is correct?

A. December 20th, at least from what is visible here.

Q. Do you believe that there are additional event log entries after December 20th, 2022 that I have failed to include in Exhibit 22?

A. I don't know. Again, I don't have the Axiom -- this is a snippet of the Axiom data case file.

Q. So when Grailer connected and disconnected her USB thumb drive to and from the computer, that created event log entries for the connections and disconnections, right?

A. It did.

Q. It did. Did you check to see whether there were any event log entries for Grailer connecting or disconnecting her USB thumb drive after December 20th, 2022?

A. That's what I'm looking at because I do

Page 233

reference in footnote the evidence of the January 8th connectivity. I am just trying to figure out --

Q. I'll tell you right now, you don't cite the event logs in your report.

A. Okay.

Q. Why don't you site the event logs in your report?

A. Because I cited the evidence of the -- what I did find of Grailer connecting that Emtec USB drive and her iPhone 6 to the work laptop on January 8th.

Q. How could Grailer have connected her thumb drive to the computer after December 20th, 2022, without causing Windows to create an event log entry documenting that connection?

A. I don't know, but if I have -- wherever -- whatever I reference, I'm not sure why you're not bringing up the evidence where I do identify the January 8th activity.

Q. We'll get to it.

But my question right now is, how could -- do you have any -- we'll back up and do it the way that seems to work.

Page 234

This is your opportunity. If you have any explanation for how Grailer could have connected her thumb drive to the computer after December 20th, 2022, without causing Windows to create an event log entry documenting that connection, tell me right now.

MR. YOSHIMURA: Objection to form.

BY THE WITNESS:

A. So it is my opinion, the evidence is consistent with the fact that a person I assume to be Jessica Grailer connected the Emtec drive to her former work laptop on January 8th, and used it to exfiltrate a significant number of Ecolab files.

Q. Do you have anything else to say about how Grailer could have possibly connected her thumb drive to the computer after December 20th, 2022, without causing Windows to create an event log entry documenting the connection?

A. Her connection of the --

MR. YOSHIMURA: Objection.

BY THE WITNESS:

A. -- connection of the Emtec drive to her laptop caused the evidence artifact that I

Page 235

described in one of my reports, one or more of my reports.

Q. Before today did you know that the event logs don't contain any entries on January 8th, 2023, showing Grailer connecting or disconnecting her thumb drive?

A. I analyzed all the evidence on the laptop. I went through each of the categories in the Axiom database. I also used OSForensics to analyze the same laptop --

Q. So you did know?

A. -- to come to the conclusion that I described in my report which is that a person I assume to be Jessica Grailer connected the Emtec drive to her work laptop on January 8th that's independently verifiable and replicatable by any qualified peer and the fact that she used that -- it is my opinion that she used that drive to exfiltrate the files that I described in my reports.

Q. So you did review all of the evidence. You did know that there were no event log entries on January 8th, 2023 for her thumb drive?

MR. YOSHIMURA: Objection to form.

Page 236

BY THE WITNESS:

A. I analyzed each category of evidence that in the Axiom database and my OSForensics database and formed the opinions, the basis for my opinions that I describe in my expert reports.

Q. You said earlier when Grailer connected and disconnected her USB thumb drive that would cause updates to the USBSTOR sub key in the Windows registry, right?

A. I said a human action of plugging in a USB drive to a Windows computer can leave evidence of activities in multiple locations on a Windows computer.

Q. Is one of those locations the USBSTOR sub key?

A. It can.

Q. Is it or can it be?

MR. YOSHIMURA: Objection to form.

BY THE WITNESS:

A. So, again, I'd like to see my specific -- so I can be specific in my responses, my expert report where I describe the activities on January 8 because the evidence that I cite in my footnote can be independently verified and replicated by

Page 237

any qualified peer.

Q. Do you know whether or not within the USBSTOR sub key hierarchy there is a specific sub key that has a timestamp for the last time Grailer's USB thumb drive was inserted into the computer?

A. I do recall that Magnet Forensic Axiom actually pulls out first insertion, last insertion, and a variety of timestamps.

Q. Including from the USBSTOR sub key?

A. It could be. Again, you're asking me a very specific question. I don't have my report in front of me. I would like to have that report in front of me so I can answer your question specifically as to how I formed that opinion for January 8th, which is my opinion.

Q. Do you know whether or not in the USBSTOR sub hierarchy there is also another specific sub key that has a timestamp for the last time Grailer's thumb drive was removed from the computer?

MR. YOSHIMURA: Objection.

BY THE WITNESS:

A. It could be. Again, I don't have the

Page 238

Axiom or OSForensics database in front of me. If I did, I could bring that up on the screen and show you exactly where I see the evidence of her activities on January 8th, which can be independently verified by any qualified peer.

Q. Do you know whether or not when Grailer connected and disconnected her USB thumb drive the last insertion and last removal timestamps would automatically update in the USBSTOR sub key?

MR. YOSHIMURA: Objection.

BY THE WITNESS:

A. I don't understand the question. Say it again.

Q. Do you know whether or not when Grailer connected and disconnected her USB thumb drive there were last insertion and last removal timestamps that would update automatically in the USBSTOR sub key?

A. I'd have to test that.

MR. YOSHIMURA: Objection.

BY MR. SPLITEK:

MR. SPLITEK: I'm going to hand you Exhibits 23 and 24.

Page 239

(Deposition Exhibit Nos. 23 and 24 were introduced to the witness.)

BY MR. SPLITEK:

Q. Exhibit 23 is a screenshot of information from your Axiom case, and then Exhibit 24 -- I'm sorry, here is Exhibit 24 -- Exhibit 24 is a zoomed-in enlargement of the right-hand column of Exhibit 23 because I think we can all see it is not very legible.

A. Okay.

Q. So first, in the middle column of Exhibit 23, there are yellow and purple, can I call them, tags --

A. Yes.

Q. -- next to several rows?

Did you put those there?

A. Unless Bruce Pixley added additional tags, I believe they're my tags.

Q. Okay. And what does yellow mean, do you know?

A. Usually it's of interest.

Q. All right. And what does purple mean?

A. I don't recall, as I sit here.

Page 240

Q. Okay. So if you look at the -- let's go to Exhibit 24, please.

A. Okay.

Q. Under evidence information in the middle of the page, do you see file paths after location?

A. I do.

Q. And do you see that most of those file paths have USBSTOR in the folder path?

A. They do.

Q. Okay. Including the file paths that end in 0066, 0067, 0064, and 0065, right?

A. Yeah, I see the writer references, yes.

Q. Okay. Having reviewed that, can you tell me whether or not in Exhibit 24 Axiom is reporting information from the USBSTOR registry sub key?

A. Yes, it appears to be.

Q. Okay. And Axiom reports a last insertion date?

A. Yes.

Q. And what date does it report on Exhibit 24?

A. Exhibit 24 it says "last insertion date

Page 241

of December 20th, 2022."

Q. Okay. And can you tell from the serial number on Exhibit 24 that what it is reporting is the last insertion date for Grailer's Emtec USB thumb drive that you discuss in your report?

A. Yes, I believe that is the Emtec drive.

Q. All right. And what is the last removal date that Axiom reports in Exhibit 24?

A. December 20th, 2022.

Q. And you obviously reviewed this information because you flagged it as "of interest" in your Axiom case, right?

A. I did.

Q. Okay. So you Axiom is reporting that last insertion date and last removal date both on December 20th of 2022 in Exhibit 24?

A. It is.

Q. Do you know how to manually check whether those timestamps are being reported accurately?

A. Well, yes.

Q. How?

A. What I do personally is I actually open up the source file and look at the entry for the

Page 242

date and time value and then I will swipe it, and then usually those date and timestamps are recorded in seconds or milliseconds from January 1, 1970 so I have another tool that will decode that to give me a time and date stamp. That's how I do it.

Q. And if we look at these hyperlinks in the middle of the page on Exhibit 24 under evidence information --

A. Okay.

Q. -- do you know what you can do by clicking on those hyperlinks?

A. Yes. If one were to click on those, it would open up the registry viewer view of Axiom.

Q. And do you know if it allows you to manually access and verify the underlying evidence relating to these timestamps that are being reported at the top of Exhibit 24?

A. It does.

Q. It does. Do you know which of the hyperlinks will take you to the underlying evidence for the last insertion date/time that Axiom was reporting as December 20th, 2022, in Exhibit 24?

Page 243

A. As I sit here, I don't know which of these blue hyperlinks devices would contain that specific value.

Q. Okay. Do you know if it might be the hyperlink ending in 0066?

MR. YOSHIMURA: Objection.

BY THE WITNESS:

A. I don't know.

Q. Do you know which hyperlink to click on to manually find the underlying timestamps that Axiom is reporting is the last removal date/time?

A. I don't have it memorized.

Q. Do you know if it's the hyperlink ending in 0067?

MR. YOSHIMURA: Objection.

BY THE WITNESS:

A. I don't know, as I sit here.

Q. Did you manually click on those hyperlinks and verify the timestamps that are shown here in Exhibit 24?

A. I don't recall if I did or didn't.

Q. All right. How could Grailer have connected her USB thumb drive to her computer after December 20th of 2022, without causing an

Page 244

update to the last insertion or last removal timestamp that Axiom is reporting here in Exhibit 24?

A. Again, I'm not sure why you're not referring to my expert report where I actually reference the evidence on the laptop that shows the evidence of activity relating to the Emtec drive on January 8th. I'm not sure why you're hiding that.

Q. Well, I want you to -- we will get to what you want to talk about. But I need answers to my questions. And so we're going to do this the other way, again.

This is your opportunity to tell me. So tell me now if you have an explanation. This is your opportunity to tell me if you have any explanation for how Grailer could connect her USB thumb drive to her computer after December 20th of 2022, without causing updates to the last insertion and last removal timestamps that are reported in Exhibit 24.

MR. YOSHIMURA: Objection to form.

BY THE WITNESS:

A. That question makes no sense to me.

Page 245

But I do recognize this exhibit as coming from the Axiom case that I generated myself, and I also know that there's evidence on the laptop of activity on January 8th that for some reason you're hiding.

Q. Do you have anything else that you want to offer about how she could connect her thumb drive after December 20th without causing updates to timestamps in Exhibit 24?

A. That question doesn't make any sense to me. But I will state that wherever it is, in one of my declarations, I provide independently verifiable evidence of Grailer connecting the Emtec drive to her former work laptop on January 8th concurrent with her activities to -- of exfiltration, in my opinion.

Q. The last insertion and last removal timestamps, do you know what form those timestamps are stored in?

A. I'm not sure what you mean by "form."

Q. What do they look like?

A. From my experience, timestamps in Windows operating systems are stored in -- it's either seconds or milliseconds since January

Page 246

1, 1970. So generally they start with 1644578, whatever. It's seconds or milliseconds since January 1, 1970. That's the form it's actually stored in.

Q. Is it stored in -- as an 8-bit hex value?

MR. YOSHIMURA: Objection; leading.

BY THE WITNESS:

A. An 8-bit hex value. So -- I mean, it's ultimately stored in zeros and ones on the hard drive.

THE VIDEOGRAPHER: I'm sorry, we need to go off the record.

MR. SPLITEK: We need to go to another volume?

THE VIDEOGRAPHER: Yeah. The time is 3:22 p.m. and we are going off the record.

(Whereupon, a discussion was had off the record.)

THE VIDEOGRAPHER: The time is 3:36 p.m. and we are back on the record.

BY MR. SPLITEK:

MR. SPLITEK: I'm going to hand you first Exhibit 25 and then Exhibit 26.

Page 247

(Deposition Exhibit Nos. 25 and 26 were introduced to the witness.)

BY MR. SPLITEK:

Q. Exhibit 25 is another screenshot taken from your Axiom case.

A. Yes.

Q. And Exhibit 26 is a zoomed-in enlargement of the right-hand column --

A. I see that.

Q. -- of Exhibit 25.

A. Yes.

Q. All right. In Exhibit 26, have we now gotten to the timestamp that you site in your report in support of your claim that Grailer connected her thumb drive to the computer at 9:39 p.m.?

A. Yes.

Q. Okay. And I want to be specific here.

A. I want to be specific too.

In my rebuttal to Mr. Pixley's report, I noted that on January 8th my forensic analysis of the Windows operating system showed that the laptop had been rebooted and restarted because

Page 248

Mr. Pixley, in his rebuttal to my report, said, how is it possible that the USB drive and the Emtec USB drive and the iPhone 6S could be plugged in at the exact same time, and I provided the evidence of that, which I have not seen Mr. Pixley rebut, which was that the forensic analysis of the Grailer laptop showed that the Windows system was restarted, and that if these USB devises, the USB Emtec drive and the iPhone were connected concurrently when the laptop was rebooted, it would be consistent with the evidence we're seeing here.

Q. And I'm sorry, would the connection time be the time of the reboot? I'm confused. When did the reboot happen? The timestamp here on Exhibit 26 is 9:39:51 p.m.

So when was the reboot then that you're talking about?

A. I don't have my rebuttal to Mr. Pixley's report, but it's -- that date and time is listed in there.

Q. But I guess just to -- I don't think we need your rebuttal for that explanation to make sense.

Page 249

Would the reboot be at 9:39:51 p.m., would it be before 9:39:59 or sometime after?

A. The system restart is at the time and date that's described in my response to Mr. Pixley's report.

Q. But that's not -- you brought this up. I wasn't going to ask you about this.

But are you saying a system reboot earlier in the day on January 8th, 2023, could cause all of the timestamps to be identical later in the day?

A. Mr. -- no. Mr. Pixley's rebuttal to my report, he criticized my findings saying how is it possible that someone could plug in a USB drive, as I describe, and an iPhone 6S within microseconds of each other. I don't have his report in front of me, but that's basically my recollection of his language.

And in response to that I did analysis and produced a subsequent report that showed that the reasonable explanation was -- was that a Windows systems had been restarted. That's what the evidence shows and did result, in my opinion, with the evidence that we're seeing here.

Page 250

Q. So let's just look at Exhibit 2, your report, paragraph 17.
A. I have two Exhibit 3s. This must be yours.
I'm looking for Exhibit 2. Got it.
Q. Okay. So in your Exhibit 2 in paragraph 17 --
A. Okay.
Q. -- you say that Grailer last connected her Emtec thumb drive at 9:39:51 p.m. on January 8th, 2023, right?
A. That is what it says.
Q. Okay. And do you believe that at 9:39:51 p.m. on January 8th, 2023, Grailer connected her thumb drive to her laptop?
A. That's what the Windows system entry had recorded.
Q. Okay. And then you were talking about a different timestamp as well for the iPhone, right?
Okay. So now let's go to Exhibit 8. This is your February declaration.
A. Okay.
Q. In paragraph --

Page 251

A. Hold on.
Q. Sorry.
A. I got it.
Q. Actually let's look at paragraph 20. In paragraph 20 of your February declaration, you said that Grailer last attached her iPhone to her laptop at that exact same time, 9:39:51 p.m. on January 8th, 2023, right?
A. That is what the evidence shows.
Q. Okay. So you're saying that she simultaneously connected both her USB drive and her iPhone to the laptop at 9:39:51 p.m. on January 8th, 2023?
A. What I'm saying is that the forensic analysis revealed Jessica Grailer last attached her iPhone 6S, serial number 9&30A71D7&1&0000 to the laptop on January 8th, 2023 at 9:31:51 p.m. And I cite the Windows system hive, the Enum, which is E-N-U-M, slash, USB registry entry.
Q. So the time that you give for when she last connected her USB thumb drive is 9:39:51 p.m. on January 8th, 2023, right?
A. I have not encountered any evidence that changes my opinion that are in my reports and

Page 252

these date and timestamps are wholly consistent with my opinion that Jessica Grailer exfiltrated the files I detailed on January 8th using either the Emtec drive or the iPhone 6S which were connected to the laptop on the evening of January 8th.
Q. And they were both connected at the same second, according to the timestamps you've given us, right?
A. And the timestamps -- sorry, go ahead.
Q. And you contend those timestamps are accurate?
A. I have no evidence -- I found no evidence to show that these timestamps are not accurate.
Q. So I guess if you're contending, though, that she actually simultaneously connected both devices to her computer at 9:39:51 p.m. on January 8th, 2023, what are you trying to explain?
Your opinion is that she connected them both to the computer at that time. Isn't that your explanation?
A. The evidence that can be independently verified by any qualified peer shows that both the

Page 253

iPhone 6S and the Emtec drive were connected to the Jessica Grailer laptop on January 8th, at 9:39 p.m.
Q. And 51 seconds?
A. And 51 seconds.
Q. Okay. In Exhibit 26 -- Exhibit 26 is showing us the timestamp that you site in support of your claim that Grailer connected her iPhone to her computer at 9:39:51 p.m. on January 8th, 2023, right?
A. It is.
Q. Okay. Do you believe that Grailer first installed her thumb drive on the computer at 9:39:51 p.m. on January 8th, 2023?
A. I don't understand that question.
MR. SPLITEK: Can you read it back to him.
(Whereupon, the record was read as requested.)
BY THE WITNESS:
A. I don't understand the question because software programs are installed on a computer, not USB drives.
Q. All right. So look at Exhibit 26. Do

Page 254

you see first install date/time?

A. I do.

Q. And do you see it is the identical January 8th, 2023, 9:39:51 p.m.?

A. I do.

Q. What is that telling us?

A. In my opinion, the evidence is consistent with the fact that a person I assume to be Jessica Grailer connected the -- and had connected the Emtec drive and her iPhone 6S to her work laptop the evening of January 8th, which is consistent with the evidence of interacting with and exfiltrating the files I described in my report.

Q. And according to Exhibit 26, when is the last time Grailer removed her thumb drive from the computer?

A. The registry value says last removal date and time January 8th, 2023 9:39:51 p.m.

Q. Do you contend that timestamp accurately reflects when she last removed the thumb drive from the computer?

A. It's my opinion that the person I assume to be Jessica Grailer had this Emtec drive

Page 255

connected to her work laptop on the evening of January 8th at 9:39 p.m., which is consistent with the activity of accessing and, in my opinion, exfiltrating the files described in my export report.

Q. So Exhibit 26 says that she both inserted the thumb drive into the computer at 9:39:51 and also removed the thumb drive from the computer at 9:39:51.

Do you believe that both of those are accurate?

A. It is my opinion that Jessica Grailer connected this Emtec drive to her former work laptop on the evening of January 8th, 2023, and her iPhone 6S and used one or both of the devices to exfiltrate the files that are described in my expert report.

Q. And then she did that after 9:39:51 p.m., correct?

A. It's my opinion that Jessica Grailer used this Emtec drive and/or the iPhone 6S which were connected to the laptop on the evening of January 8th, 2023, to exfiltrate the files addressed in my report.

Page 256

Q. Not my question.

So the timestamp there, 9:39:51 p.m. on January 8th, 2023, do you see that?

A. I do.

Q. Did the exfiltration that you allege occur before or after that specific time?

A. I believe the evidence shows that Jessica Grailer exfiltrated the files that I described in my expert report on the evening of January 8th, 2023, using the Emtec USB drive and/or the iPhone 6S that was connected to her laptop that evening.

Q. So if you look at Exhibit 26, the only timestamp that is given is 9:39:51 p.m. on January 8th, 2023, right?

A. Yes.

Q. Do you understand so far?

A. I see those timestamps.

Q. And you allege that Grailer exfiltrated files to her USB thumb drive, right?

A. Or the iPhone 6S, as the evidence shows that both devices were connected to her laptop on the evening of January 8th concurrent and consistent with the evidence of the file

Page 257

exfiltration.

Q. So my question to you is: Do you claim that that file exfiltration happened before or after you say that Grailer connected her USB thumb drive to the computer at 9:39:51 on January 8th, 2023?

A. It is my opinion that Jessica Grailer connected the Emtec drive and her iPhone 6S to her Ecolab laptop on January 8th, 2023, and used one or both of those devices to exfiltrate the files described in my expert report.

Q. Okay, I understand that. I guess I have a different question, though, which is: Do you claim that the exfiltration you just referred to happened before or after 9:39:51 p.m. on January 8th, 2023?

A. So I'm reading paragraph 18, page 5.

Q. Of what?

A. Of Exhibit 2.

[As read]: Forensic analysis. The Ecolab laptop revealed Jessica Grailer accessed and exfiltrated multiple files on January 2023 -- January 8th, 2023, including the 259 files described in Exhibit E based on -- should be my

Page 258

forensic analysis.
[As read]: It is my opinion that the 259 files were copied by Jessica Grailer to the Emtec drive on January 8th, 2023.
I found no evidence to change my opinion.
Q. All right. So you just directed me to paragraph 18 of your report in Exhibit 2, right?
A. Yes.
Q. Okay. And you talked about the exfiltration that you say happened in that paragraph, right?
A. Yes.
Q. So I have a related question for you.
The exfiltration that you're talking about in paragraph 18 of your report, is it your opinion that that exfiltration happened before or after 9:39:51 p.m. on January 8th, 2023?
A. I don't know. I'd have to look at the access dates and timestamps on the files that I described as her being exfiltrated.
Q. So you don't know?
A. I do know. I know that the files that were -- that identified as being exfiltrated all

Page 259

have date and timestamps that are consistent with my opinion that Jessica Grailer connected an Emtec USB drive to her former work laptop on the evening of January 8th, 2023, and exfiltrated the files that I described.
Q. How could Grailer have exfiltrated files to her thumb drive before connecting her thumb drive?
A. I don't see anywhere in my report where I claimed that. I am not claiming that.
Q. Okay. So you don't claim that she exfiltrated files before you say she connected her USB thumb drive at 9:39:51 on January 8th, 2023, correct?
A. It is any opinion that the evidence shows that the Emtec USB drive was connected to Jessica Grailer's Ecolab laptop on the evening of January 28, 2023, which is consistent with the dates and timestamps that I see on the files that I describe as her having exfiltrated.
Q. And you don't claim, of course, that she somehow exfiltrated files to her thumb drive before connecting it?
A. If you're asking me if files can be

Page 260

copied to a USB drive that is not connected to a laptop, is that what you're asking.
Q. That is, yes.
A. That's impossible.
Q. All right.
And you would agree with me that in paragraph 17 of your report, the only time of connection that you identify is 9:39:51 p.m. on January 8th, 2023, correct?
A. Yes. It's my opinion that the system hive of the laptop under the Enum/USB registry entry contains evidence of Jessica Grailer having had this Emtec drive connected to her laptop on January 8th 2023.
Q. Do you know if the timestamps that Axiom is pulling out here on Exhibit 26 are coming from what I referred to before as the USB sub key?
A. Well, I'm looking at the -- what they say is the source is the system hive, and it's saying -- it shows the location as control set 1 Enum/USB, Enum/USB. That's what I cite. That's exactly what I cite in my expert report.
Q. And you can click on the hyperlinks shown in Exhibit 26 to verify the timestamps that

Page 261

are being recorded in Exhibit 26, right?
A. One can, yes.
Q. Did you?
A. Yes.
Q. You did. And what did you find? Did they match the timestamps reported in Exhibit 26?
A. That is my recollection.
MR. SPLITEK: I'm going to hand you Exhibit 27.
(Deposition Exhibit No. 27 was introduced to the witness.)
THE WITNESS: Okay. Well, give me the blown-up version.
MR. SPLITEK: Yep. And I'm also going to hand you Exhibit 28 --
(Deposition Exhibit No. 28 was introduced to the witness.)
MR. SPLITEK: -- which is an enlarged version of the right-hand column of Exhibit 27.
THE WITNESS: Okay.
BY MR. SPLITEK:
Q. So if we go back to Exhibit 26, you can click on the hyperlink ending in 0066, right?

Page 262

A. 00 -- yes.

Q. Okay. And that will take you to the underlying timestamp that is being reported above at the top of Exhibit 26, right?

A. I'm not -- I have not clicked on this particular item, but -- so I see that Windows decoding it as 12:20, 2022.

Q. That's right. But I thought you said you did click on the hyperlink shown in Exhibit 26 to manually access the underlying timestamps.

A. Yeah, I recall confirming these dates and that they are accurate and can be independently verified by any qualified peer.

Q. So the timestamp that Axiom is pulling from the sub key ending in 0066, it is one of the timestamps that comes in on January 8th, 2023, at 9:39:51 p.m., right?

A. So I didn't create this Exhibit 28. But if I had the Magnet Forensics Axiom case database in front of me, I could pull up what I bookmarked here as this particular evidence you're showing as Exhibit 26 and I could show you where the timestamp is deriving from.

Q. But that's just a factual question and

Page 263

our expert too can click on the hyperlink.

What I'm telling you is that when you navigate from the hyperlink for the sub key ending 0066 and you decode the value, Axiom reports December 20th, 2022, is the timestamp, not January 8th.

MR. YOSHIMURA: Objection to form, foundation.

BY MR. SPLITEK:

Q. Assuming that's true, do you have any explanation for why the timestamp that Axiom is reporting in Exhibit 28 would not have been updated after December 20th of 2022?

MR. YOSHIMURA: Objection; form, foundation.

BY THE WITNESS:

A. Yeah, I didn't generate Exhibit 28. It is a window within -- appears to have been derived from an Axiom case file.

It is my opinion that -- and the evidence is consistent with the fact that Jessica Grailer connected this Emtec USB drive to her work laptop on January 8th and used it to exfiltrate the files described in my report.

Page 264

Q. So in Exhibit 26, that last insertion timestamp of January 28th, 2023, 9:39:51 p.m., I think what you're telling me is you don't know when you go in to manually access the underlying timestamp whether it turns out to match the January 8th, 2023, 9:39:51 p.m. timestamps or not, right?

A. No, I didn't say that.

MR. YOSHIMURA: Objection.

BY MR. SPLITEK:

Q. So you do know?

A. I said that the evidence reported here by Axiom and in my expert report is consistent with the fact that Jessica Grailer connected this Emtec drive to her laptop on the evening of January 8th, and, in my opinion, used it to exfiltrate the files described in my report.

Q. And if you look at the last removal timestamp shown on Exhibit 26, do you know whether or not you can manually validate that by navigating through the hyperlink for the sub key ending in 0067?

MR. YOSHIMURA: Objection.

Page 265

BY THE WITNESS:

A. I'm not sure I understand the question.

Q. So just like Axiom in Exhibit 26, it reports the same timestamps for all the events, right?

A. Okay.

Q. Well, it does?

A. It does. I see that.

Q. So the last one, because Axiom reports that Grailer first installed, last inserted and last removed her USB all at the same second, right?

A. Okay.

Q. The last timestamps for last removal of January 8th, 2023, 9:39:51 p.m., do you know whether or not the underlying timestamp for that report is stored at the sub key ending in 0067, which you can see a hyperlink for in Exhibit 26?

MR. YOSHIMURA: Objection.

BY THE WITNESS:

A. As I sit here, I don't know which of these particular hyperlink entries correlate with the entries described above.

MR. SPLITEK: I'm going to hand you

Page 266

Exhibit 29.

(Deposition Exhibit No. 29 was introduced to the witness.)

MR. SPLITEK: And I'm going to hand you Exhibit 30.

(Deposition Exhibit No. 30 was introduced to the witness.)

BY MR. SPLITEK:

Q. Exhibit 29 is another screenshot from your Axiom case and Exhibit 30 is an enlargement of the right-hand column of Exhibit 29.

I will represent to you that when you click on the hyperlink for the sub key ending in 0067 in your Axiom case and decode the timestamp, the value, again, comes back as December 20th, 2022.

Assuming that's true, do you have any explanation for why that happens?

MR. YOSHIMURA: Objection; foundation.

BY THE WITNESS:

A. So I didn't create Exhibit 30 and I'll note that in my footnote to Exhibit 2, footnote No. 2, it lists the source as system control set 001/Enum/USB and has a vendor ID and product ID

Page 267

related to this device, and then a serial number.

This particular exhibit has a different location; it ends in 0067. So you're citing here a different location from what I'm citing.

Q. Do you know whether or not that timestamp corresponds -- let me be specific here.

Do you know whether or not the timestamp shown in Exhibit 30 corresponds to the last removal date/time that is reported in Exhibit 26?

MR. YOSHIMURA: Objection.

BY THE WITNESS:

A. I didn't create this timestamp, but I will say that I've found no evidence that the timestamps in Exhibit 26, which correlate with my expert report, page 5, paragraph 17, are incorrect.

Q. And you also used your OSForensics software to double-check the timestamps that you found in Axiom, right?

A. I used OSForensics tool to process and make a case out of the laptop, but I don't believe -- I could be wrong -- I don't believe I reference OS -- evidence from OSForensics here. I'm looking

Page 268

here, this -- at paragraph 17 and my recollection is that is coming from my analysis that I performed using the Axiom database.

Q. Did you -- I understand what you did and didn't cite in the report.

But did you use OSForensics to review any of the information it provided about when Grailer connected and disconnected her USB thumb drive?

A. I don't recall.

MR. SPLITEK: I'm going to hand you Exhibit 31.

(Deposition Exhibit No. 31 was introduced to the witness.)

BY MR. SPLITEK:

Q. So you did not provide us a copy of your OSForensics case, right?

A. I don't recall if I did or didn't. It is possible. I just don't recall.

Q. I will represent to you that Bruce Pixley used OSForensics himself to extract information from the image of Grailer's laptop.

A. Okay.

Q. And you did the same thing, right?

Page 269

A. I did process the forensic image of Grailer's laptop using OSForensics.

Q. All right. So here in Exhibit 31, it shows what OSForensics reports -- if you go to first the "user activity" section and then if you look at the next column under USB near the bottom, it's the "US devices" section.

Do you see that?

MR. YOSHIMURA: Objection --

BY MR. SPLITEK:

Q. Sorry. "USB devices" section.

MR. YOSHIMURA: Objection; foundation.

BY MR. SPLITEK:

Q. Well, I'm just asking about looking at the document here.

So in the left-hand column, "user activity" is highlighted and then the second column near the bottom under USB, what's highlight is "USB devices."

Do you see that?

A. I do.

Q. Okay. Do you remember reviewing USB devices information like this in OSForensics?

A. I don't recall.

Page 270

Q. Okay. So in Exhibit 31, we can find entries, again, for Grailer's thumb drive, right?

MR. YOSHIMURA: Objection.

BY THE WITNESS:

A. Sorry. I don't understand the question. This is hard to read.

Q. Well, I made it big in an effort to --

A. Yeah, sorry for not bringing glasses.

Q. About halfway down the page there are three entries. One says, VID_6557 PID_4200, and then the next two are USB disc 2.0 and USB disc 2.0.

Do you sees though entries?

MR. YOSHIMURA: Objection.

BY THE WITNESS:

A. I believe so. USB disc 2.0?

Q. That's right.

A. Okay.

MR. YOSHIMURA: Matt, just for the record, I have to state an objection to this to the extent that unlike the other screenshots that you showed us, this is not based on processing that has been done by both parties. We cannot independently

Page 271

confirm this on our end after this deposition and we object to its usage.

MR. SPLITEK: Are you going to give us his OSForensics case then?

MR. YOSHIMURA: I don't believe that that has anything to do with the objection I just raised. And if you and I want to meet and confer about that, we can.

I don't think that needs to be answered on the record in this deposition.

MR. SPLITEK: All right.

BY MR. SPLITEK:

Q. But in any event, you provided the image of Grailer's laptop, right?

A. I did.

Q. And another independent expert is able to use OSForensics to extract information from it, right?

A. I used OSForensics to extract information from the Grailer laptop, which I describe in my most recent expert report.

Q. But if two people both use OSForensics from the same image, the information that OSForensics extracts shouldn't be different,

Page 272

right?

A. I don't know if it is -- which version did he use?

Q. It could be a more recent version than yours. That would be likely.

MR. YOSHIMURA: Objection.

BY MR. SPLITEK:

Q. Do you see in the serial number column?

A. Okay.

Q. Do you see entries there, serial number ending in 070 -- I'm sorry, beginning in 070?

A. I'm having a difficult time reading this; it is so small. I see date last connected. Oh, gosh, I can't read it.

Q. All right.

A. I really can't.

Q. Do you have any reason to dispute that when somebody uses OSForensics to extract the USB device's information from the image of Grailer's laptop they are told that Grailer's USB thumb drive was last connected on December 20th, 2022?

A. I don't understand the question.

So the Axiom database shows evidence of this Emtec drive being connected on December 20th,

Page 273

2022. I address that in my report. The Axiom database shows evidence of Grailer also connecting the same Emtec drive to the Ecolab laptop on January 8th, 2023. I address that in my report.

Q. I guess what I'm telling you is, I'm representing to you that when someone uses OSForensics to extract the information shown in Exhibit 31, they are told that Grailer's USB thumb drive was last connected on December 20th, 2022.

And all I'm asking is just sitting here today, do you have any reason to dispute that that is, in fact, what OSForensics reports?

MR. YOSHIMURA: Objection.

BY THE WITNESS:

A. I have not generated this particular exhibit. I will state that I have no reason or I found no evidence to -- that the evidence reported in Exhibit 26 on January 8th is incorrect.

Q. All right.

MR. SPLITEK: I'm going to hand you Exhibit 32.

(Deposition Exhibit No. 32 was introduced to the witness.)

MR. YOSHIMURA: For the record, we'll

Page 274

make the same objection. Exhibit 32 appears to be derived from another source, the same source as Exhibit 31.

BY MR. SPLITEK:

Q. So I will represent to you that the information shown in Exhibit 32 was extracted from the image of Grailer's laptop that you provided using OSForensics software, and that as depicted in Exhibit 32, this is now the USB history information that OSForensics reports.

A. Okay.

Q. If you look at just what's on the face. I'm not asking you to agree that OSForensics is right, but if you look at the face of Exhibit 32, when is the -- when are the last connection and disconnection events that you see for Grailer's USB thumb drive?

MR. YOSHIMURA: Objection.

BY THE WITNESS:

A. According to this report, it says December 20th, 2022, and this is reporting it from the diagnostic event log, which is different from the source I quote in paragraph 17 of my report.

Q. And do you have any explanation for how

Page 275

Grailer could have connected her thumb drive to the laptop after December 20th, 2022, without causing another entry in that log?

MR. YOSHIMURA: Objection.

BY THE WITNESS:

A. I don't need to. I found forensic analysis of the laptop showed that Grailer connected the Emtec drive to her laptop -- to the Ecolab laptop on the evening of January 8th, 2023.

Q. By the way, on Exhibit 32, who was connecting USB devices on February 8th?

MR. YOSHIMURA: Objection.

BY THE WITNESS:

A. That was me as part of doing the forensic imaging of the device.

Q. You had the computer running before you imaged it?

A. Yes, because it was BitLocker encrypted. My recollection is that the serial number was not visible, so I had to perform a live forensic image.

Q. Okay. And that did cause some changes in the laptop, right?

A. Specifically it caused the entries

Page 276

we're seeing here on February 8th.

Q. It also caused USN change journal entries, right?

A. I'm not aware of any.

Q. Did you check?

A. No.

Q. And the USN change journal has a maximum size, right?

A. I don't know.

Q. Do you know if when a USN change journal has a maximum size, new entries in the change journal will cause old entries to purge out?

A. I do not.

Q. All right. So you don't know whether when you were running the computer you were causing old change journal entries to purge out?

MR. YOSHIMURA: Objection.

BY THE WITNESS:

A. I found no evidence of that. And I did find evidence of US [sic] journals consistent with the January 8th exfiltration of files that I reported on.

MR. SPLITEK: I'm going to hand you

Page 277

Exhibit 33.

(Deposition Exhibit No. 33 was introduced to the witness.)

MR. YOSHIMURA: Same objection.

BY MR. SPLITEK:

Q. I will represent to you that, once again, Exhibit 33 depicts information that OSForensics software extracted from the image of Grailer's laptop that you provided, and specifically as depicted in Exhibit 33, we are looking at the event logs for storage device usage --

A. Okay.

Q. -- as you can see in the second column.

A. Okay.

Q. If you just look at the face of Exhibit 33, when here is OSForensics telling you that Grailer's thumb drive was last connected?

MR. YOSHIMURA: Objection.

BY THE WITNESS:

A. This is near impossible to read. I see -- I really can't read this, quite honestly. I see entries. I don't know. This is difficult to read.

Page 278

I see an entry on January 28th. I see an entry on February 8th. I can't read -- the text is too small.

Q. Well, let me just ask a general question.

Do you have any explanation as to how Grailer could have connected her USB thumb drive to the laptop after December 20th, 2022, without causing an additional entry in the storage device usage event logs that OSForensics reports?

MR. YOSHIMURA: Objection.

BY THE WITNESS:

A. I don't really understand the question.

I will state that I did find through forensic analysis that Jessica Grailer connected her Emtec drive to her Ecolab laptop on January 8th, 2023, as reported by my -- as described in my report and as shown in your Exhibit 26.

Q. And in Exhibit 26, do you have any explanation as to why Axiom reported identical timestamps for the last connected daytime, install daytime, first install daytime, last insertion daytime and last removal daytime?

MR. YOSHIMURA: Objection; asked and

Page 279

answered.

BY THE WITNESS:

A. I do not.

Q. What did you say?

A. I do not.

Q. Thank you.

Tell me if you agree or disagree with this statement. Axiom retrieves timestamps for USB devices from the device registry. Is that true so far?

MR. YOSHIMURA: Objection.

BY THE WITNESS:

A. Yes.

Q. And due to the behavior of registry keys, those timestamps may not always accurately reflect the true time when a user performed a certain action.

Do you agree or disagree with that?

MR. YOSHIMURA: Objection.

BY THE WITNESS:

A. Could you repeat that?

Q. Yes.

Due to the behavior of registry keys, those timestamps may not always accurately reflect

Page 280

the true time when a user performed a certain action?

A. I don't really understand what that means, but I will state that my forensic analysis of the Grailer laptop using Axiom revealed evidence of Grailer connecting the Emtec drive to her work laptop on January 8th, 2023, as described in my report.

Q. All right. Tell me if you --

A. I found no evidence and I've been shown no evidence that is incorrect.

Q. Tell me if you agree or disagree with this next statement. Timestamp data for a registry key may update when any of the data within that key changes.

MR. YOSHIMURA: Objection to form.

BY THE WITNESS:

A. I don't know. I'd have to -- it sounds like you're asking a hypothetical that would require testing.

Q. All right. You don't know. Okay.

Tell me what you think about the next statement. If multiple timestamps are recovered from the same registry key, they may all

Page 281

inaccurately display the same timestamp; for example, the one that was most recently recorded for that key.

MR. YOSHIMURA: Objection; form.

BY THE WITNESS:

A. I don't even understand what that means.

Q. Okay. Tell me what you think about this next statement. Typically an examiner needs to collect details from multiple locations to analyze USB activity on a Windows PC.

MR. YOSHIMURA: Objection; form.

BY THE WITNESS:

A. I analyzed Grailer's laptop using two different forensic tools and I was able to identify the evidence described in Exhibit 26 of Grailer connecting the Emtec drive to the laptop on January 8th, 2023, which is consistent with the timestamps we see on the files that I'm describing as having been exfiltrated.

Q. All right. So let's say that Grailer connected her thumb drive to her laptop at 9:39:51 p.m. on January 8th, 2023, which is what you're claiming, right?

Page 282

A. That's what the evidence shows.
Q. Would you expect that connection to cause changes to USB sub keys that had nothing to do with the thumb drive?
A. I don't understand the question.
Q. So if -- there are lots of sub keys in the registry, right?
A. Okay.
Q. Do you agree with that?
A. The registry has many, many, many, many entries; hundreds, if not thousands of entries.
Q. And many sub keys that are completely unrelated to Grailer's thumb drive, right?
A. The Windows registry has a system hive, a software hive, a security hive, it has NTUSER.NET file. Those registry hives and NTUSER.NET file contain evidence of human interaction and usage of a Windows machine, including what I found here in Exhibit 26, which is evidence of Grailer connecting and using this Emtec drive with her work laptop on January 8th, 2023.
Q. And so when Grailer connected her USB thumb drive to her computer, would you expect that

Page 283

connection to cause updates to sub keys that were completely unrelated to her thumb drive?
A. I don't really understand that question. I honestly don't.
Q. Did you ever check to see how many sub keys in the registry were updated at the identical time of 9:39:51 p.m. on January 8th, 2023?
A. Did I -- sorry. Repeat the question.
Q. Yeah.
Did you ever check to see how many sub keys in the registry in Grailer's -- in the image of Grailer's laptop were updated all at the identical time of 9:39:51 p.m. on January 8th, 2023?
Mr. YOSHIMURA: Objection.
BY THE WITNESS:
A. I don't really understand that question.
I did perform analysis of the Grailer laptop and found the evidence that you have displayed here in Exhibit 26.
Q. Did you ever check to see how many sub keys with no relationship to Grailer's thumb drive were all changed at the identical time of 9:39:51

Page 284

p.m. on January 8th, 2023?
A. No, I didn't need to. And I found literally no evidence -- I was presented with no evidence that this Emtec drive was not connected to the laptop on January 8th, 2023.
Q. Do you have an opinion about how many times Grailer connected and disconnected her thumb drive from her laptop on January 8th, 2023?
A. I do not.
Q. Do you have an opinion about when Grailer last removed her thumb drive from her laptop?
A. Yes.
Q. What time?
A. It was on January 8th, 2023, according to Axiom.
Q. No. Do you have an opinion about what time Grailer last removed her thumb drive from the laptop?
A. Well, the forensic artifact here is reporting 9:39:51 p.m. on January 8th, 2023.
Q. Okay. And that's what you're relying on?
A. It is my opinion and I have not been

Page 285

shown any evidence to the contrary that Grailer connected this Emtec drive to her work laptop on January 8th, 2023, and used it to exfiltrate the files described in my report.
Q. Just to be clear, I was asking about your opinion about when she last removed the thumb drive from the computer.
MR. YOSHIMURA: Objection.
BY MR. SPLITEK:
Q. You're still pointing to the timestamp in Exhibit 26, though; am I right?
A. That's the evidence that the Axiom tool reports.
Q. Okay. So to support your claim that Grailer exfiltrated the files that you listed in your Exhibit E, you cite the USN change journal in the image of her laptop, right?
A. I did.
Q. Okay. And you cite the entire change journal; not to any specific entries there, right?
A. No. I believe in my original report I actually had the USN journal entries related to the files I described as being exfiltrated.
Q. Well, we're going to look at -- let's

Page 286

go to Exhibit 2, paragraph 18, footnote 3.

A. Okay.

Q. That's the entire USN change journal that you're citing on page 5 of Exhibit 2, right?

A. So paragraph 18 says, Forensic analysis of the --

Q. And I want to focus you on footnote 3 at the bottom of page 5.

Are you or are you not citing the entire USN change journal in footnote 3 of page 5 of Exhibit 2?

A. I don't know if you're describing as the entire USN. It says in my footnote, too, it ends $USNJRNL, I believe, it's a colon, $J.

Q. And that's the USN change journal, right?

A. It could be the entire journal. I don't know.

Q. Well, it's your footnote. I mean, is it one entry in the journal or is it the whole journal?

MR. YOSHIMURA: Objection.

BY THE WITNESS:

A. I took this from the Axiom forensic

Page 287

database. That's why I'm citing it so that any independent expert could verify that and find the same evidence at the same location on the laptop.

Q. And you would agree with me that the USN change journal does not track files being copied to external storage media, right?

A. No. I disagree.

Q. What is it -- how does it track files being copied to external storage media?

A. So USN journal files, as I describe in my report, record human interaction with files.

Q. And the -- is there a reason field in each change journal entry?

MR. YOSHIMURA: Objection.

BY THE WITNESS:

A. I don't know what that means.

Q. Okay. What -- when there's an entry in a USN change journal, what information is recorded in the entry?

A. Well, we'd have to look at each of the USN journal entries that I provided. I believe it was in my original declaration.

Q. But are you saying that in the USN change journal, entries will say this file was

Page 288

copied to external storage media?

A. What I'm something is that I referenced the USN journal entries related to the files I described as having been exfiltrated, and I included all of them in my expert report.

I was later asked to provide copies of those files to be produced. Those files all had the date -- last access date and timestamp consistent with my opinion that those files were exfiltrated via this Emtec USB drive.

Q. But I guess what I'm asking is, are you claiming that if someone goes into the USN change journal, they will see a report in there that says this file was copied to an external storage media at this time?

A. What I found through the analysis of the USN journal, which is a -- records human interaction with files, it shows the files I described as being exfiltrated were interacted with concurrent with the date and time of those files being exfiltrated.

And then when I was later asked to produce those, the date last accessed, modified, created metadata dates lined up perfectly with my

Page 289

opinion and the USN journal files. All of it is consistent.

Q. So if you go into one of these USN change journal entries that you're relying on, what kind of information would it provide to you?

A. Human interaction with those files; not a system, not automated. Human interaction.

Q. And does it tell you what kind of interaction?

A. Well, there is many different types of USN journal entries. We would have to look at the specific ones that I report on and that are available in the Axiom database.

Q. And are any of those entries about copying to external storage media?

A. I don't recall.

Q. Do you know how many entries exist in the USN change journal in the image of Grailer's laptop?

A. I do not.

Q. Could you approximate it?

A. As I sit here, no.

Q. More than 100,000?

A. As I sit here, I do not know.

Page 290

Q. Do you know when the USN change journal's earliest entry is from?

A. I don't recall.

Q. Do you know how many of the USN change journal entries are from February 8th, 2023 when you had the laptop?

A. I don't know how many, as I sit here.

Q. All right. I want to -- here's what I, you know, I don't fully understand is the chronology.

So in my mind, if somebody is copying files to a USB thumb drive, they have to connect it at some specific time.

A. Right.

Q. And then there is a period of time after the connection where the copying to the thumb drive would have to happen, right?

A. That's right.

Q. And then at the end they also remove the thumb drive.

A. I agree.

Q. Could you provide that rough chronology to me right now?

A. Yeah. So my forensic analysis showed

Page 291

that a person I believe to be Jessica Grailer connected Emtec USB drive to her former work laptop on January 8th 2023. The forensic analysis of the USN journal files showed her interacting with those same files, as I describe as being exfiltrated.

The actual metadata of those files that got produced, hopefully you have those exhibits, are all consistent with them being accessed en masse currently on the evening of January 28th, 2023.

So the timeline is self-evident in the metadata of the files that were produced as having been exfiltrated, as consistent with the entry we see here in Exhibit 26, and it is consistent with the activity we see in the USN journal. It is all consistent.

Q. Well, I'm probably not a very smart guy, but it's not all self-evident to me. So I want to break it down.

The three stages we identified were in the chronology. There's three points in this chronology I want to focus on. One was the user connects the thumb drive to the computer.

Page 292

A. Okay.

Q. And the next is a period of time where there is copying to the thumb drive, right?

A. Yes.

Q. And then the final point is the thumb drive is removed from the computer, right?

A. Yes.

Q. All right. So let's just focus on the beginning of have chronology --

A. Okay.

Q. -- which is the event where the user connects the thumb drive to the computer.

A. Okay.

Q. What is the specific time on January 8th, 2023, that you claim that chronology began?

A. So the evidence, as shown in your Exhibit 26, shows that the Emtec drive was connected to the laptop on January 28th, 2023, at 9:39 p.m., which, in my opinion, is why that activity doesn't show up in the Digital Guardian report.

And if we look at the -- I don't have the Axiom database in front of me but if we did, maybe Mr. Pixley can bring it up on screen because

Page 293

I tagged all those files that as I describe, we can see the last access dates and times are consistent with or after the connectivity of the USB drive.

So it is any opinion and the evidence is consistent with the fact that Ms. Grailer used this Emtec driver to exfiltrate the files I described in my expert report on the evening of January 28th.

Q. Okay. And just to be clear then, that chronology I referred to in my last question, in your view it began at the 9:39 p.m. timestamp that we saw in Exhibit 26, correct?

A. Yes.

Q. Okay. Are you certain that the USN change journal on Grailer's laptop contains entries relating to all of files in your Exhibit E?

MR. YOSHIMURA: Objection.

BY THE WITNESS:

A. I don't understand the question.

Q. Well, so you cite the USN change journal --

A. Yes.

Page 294

Q. -- in support of your claim that Grailer exfiltrated all of the files listed in Exhibit E to your report, right?

A. Yes.

Q. Okay. And it wouldn't make sense for you to cite the USN change journal as evidence that files were copied if the USN change journal had no entries about those files, right?

MR. YOSHIMURA: Objection.

BY THE WITNESS:

A. I don't really understand that question. But I believe it would be informative to have a copy -- maybe you have that and you're about to provide it to me. My rebuttal to Mr. Pixley because I believe I addressed that exact subject in my rebuttal to his report.

Q. About how much time did you spend analyzing the USN change journal to determine that Grailer copied the files listed in your Exhibit E?

A. I don't recall.

Q. Did you perform that analysis before executing your February 2023 declaration?

A. If I describe -- I believe so. I believe that the original declaration where I

Page 295

describe the file exfiltration was based upon my evidence of human interaction that I discovered through the identification of the USN journal entries, which are a direct result, in my opinion, of actions Jessica Grailer took.

At a later date I was asked to -- I believe Fisher Phillips said we got to produce the true and exact copies of the files that I'm describing as her having been exfiltrated, and my recollection is that the metadata dates of all of those files that are produced are completely consistent with my opinion.

Q. Which dates in the production that we received should be showing up then as January 8th, 2023, in the metadata?

A. Which what?

Q. You're saying that the metadata was consistent. Are you telling me that some date in the metadata for the production?

A. Yeah. It would be the last access dates.

Q. The last access dates in the documents that were -- that you gathered to provide to us were all January 8th, 2023?

Page 296

A. The evening of, yes. You should have that -- if you have a relativity database, you can confirm that.

Q. Okay. Did you do any analysis to rule out the possibility that programs running in the background on Grailer's computer caused USN change journal entries relating to files that are listed in your Exhibit E?

A. No. I'm not aware of any instances where automatic software -- what did you say? A Windows operating system -- so nonhuman activity would cause the evidence I saw in the USN user journals to be changed or recorded.

Q. When Grailer's laptop started up, Windows would automatically start up different kernel and file system drivers, right?

A. Say that again.

Q. Do you know whether when Grailer's laptop started up Windows would automatically start up different kernel and file system drivers?

A. What's the last word you're saying?

Q. Kernel and file system drivers.

A. Oh, kernel and file system drivers.

I don't know.

Page 297

Q. Do you know how many additional programs were also set up to start up automatically when Grailer's laptop started?

A. I don't recall doing that analysis.

Q. Okay. Do you agree that programs running in the background in the computer can interact with files without the user's intervention?

A. I am aware of antivirus programs which are running in the background will -- periodically will be -- con be configured periodically to scan files on a computer just -- and be set up to run in an automatic fashion. But I'm not aware of that occurring here.

Q. Do you agree that USN change journal entries will result when a program running in the background interacts with a file?

A. I'm not aware of any evidence or instance of that occurring.

Q. Did you check the Windows event logs to determine whether Grailer logged into the computer in close proximity to any of the USN journal entries relating to files in your Exhibit E?

A. I don't recall.

Page 298

Q. When I say "your Exhibit E," I mean Exhibit E to your report.
A. Okay.
Q. Are we on the same page?
A. I didn't really understand the question. What was the question?
Q. Yeah.
So I thought the question went well and then I tripped up by making sure we were talking -- Exhibit E to your report from November --
A. Okay.
Q. -- identifies the files that you claim Grailer exfiltrated, right?
A. Can I pull that up?
Q. Sure, yeah. That's fine.
MR. SPLITEK: Let's mark a new one. Exhibit 35 I'm handing to you.
(Deposition Exhibit No. 35 was introduced to the witness.)
BY MR. SPLITEK:
Q. Do you agree that Exhibit 5 is a copy of Exhibit E to your report?
MR. YOSHIMURA: Exhibit 35.

Page 299

BY MR. SPLITEK:
Q. Exhibit 35 is a copy of Exhibit E in your report, right?
A. If appears to be.
Q. Did you check the Windows event logs to determine whether Grailer logged into the computer in close proximity to any of the USN journal entries relating to files in your Exhibit E?
A. Did I specifically analyze Windows event log to -- I don't understand that question.
Q. All right. Did you check the OneDrive synchronization log to determine whether a OneDrive program was synchronizing files at the time of any of the USN journal entries relating to files in your Exhibit E?
A. I don't recall.
Q. Do you agree that when OneDrive synchronizes files, that will result in USN change journal entries for the synchronized files?
A. I'm not aware of that occurring.
Q. Did you check to see if any of the files listed in your Exhibit E were being written to in regular increments on the computer?
A. No. I'm only aware of evidence of USN

Page 300

journal files being created as a direct result of human activity.
Q. Did you do any analysis to determine whether USN change journal entries for files in your Exhibit E related to temporary files that were being created and deleted on January 8th of the 2023?
A. I don't recall identifying any of these as temporary files.
Q. All right. Did you check to see whether any files in your Exhibit E were temporary files located in temporary folders?
A. I don't recall any of these being temporary files or located in temporary folders.
Q. Do you recall looking to find out if they were or weren't?
A. I wouldn't have reported on a file being exfiltrated if that file originated from a temporary file.
Q. Did you do any analysis to determine whether the USN change journal entries for files in your Exhibit E related to a program called End Point Sensor that was running in the background?
A. I did not.

Page 301

MR. YOSHIMURA: Objection.
BY MR. SPLITEK:
Q. Did you do any analysis to determine whether any USN change journal entries for files in your Exhibit E were related to the Digital Guardian agent running in the background?
A. No. And I'm not aware of Digital Guardian agent having any effect on user journal files because, again, my understanding and experience with user journal files is they're created as a direct result of human activity.
Q. Did you do any analysis to identify the folder pads for all the files in your Exhibit E?
A. Oh, yes.
Q. Did you do any analysis to determine whether the files in your Exhibit E had folder locations such that a user could have plausibly selected them for copying at the times that you believe they were copied?
A. I don't recall that specifically, but I do recall identifying these files as -- and evidence that was consistent with Grailer exfiltrating these specific files on January 8th 2023.

Page 302

Q. And do you agree with me, though, that although it is easy to simultaneously select and copy multiple files that are stored together in the same folder, it's not so easy to simultaneously select and copy files that are spread out in different folders in different locations?

A. I think you're asking a hypothetical. But I know I can -- in Windows Explorer I can hit -- while the control key is held down, I can simultaneously select multiple files in different folders.

Q. But it would take you more than a second or two to do that, I assume?

MR. YOSHIMURA: Objection.

BY THE WITNESS:

A. I really don't understand the question.

Q. Did you do any analysis to determine whether USN change journal entries for files in your Exhibit E were related to thumbnails of files previewing in a folder?

A. No.

Q. Did you check to see whether any of the files in Exhibit E are just files that Grailer

Page 303

sent or received by e-mail on January 8th, 2023?

A. No.

Q. And if Grailer sent or received files by e-mail, there would be USN change journal entries relating to those files, right?

A. I don't know that.

Q. Okay. But you did have access to all the e-mails Grailer sent or received on January 8th, 2023, right?

A. I had access to all the e-mails Grailer received using her laptop.

Q. Okay. But you didn't check to see whether in your Exhibit E you might be accusing her of exfiltrating files that she just sent or received in her work e-mail?

MR. YOSHIMURA: Objection.

BY THE WITNESS:

A. I found no evidence of Grailer e-mailing the files that I identified in Exhibit E, your Exhibit 35, as result -- a direct result of her sending an e-mail to another Ecolab employee or herself via an e-mail attachment. Because if I had, I would not have identified that file as a file I believe she exfiltrated.

Page 304

Q. Can you go back to Exhibit 36, which is Exhibit F to your report?

A. Exhibit 36.

Q. I want you to turn to page 2 of Exhibit 36 --

A. Okay.

Q. -- which, again, is your Exhibit F.

A. Okay.

Q. At the bottom of the page do you see the shortcut to a file with a name that begins with .849C9?

A. I do.

Q. Do you know what that file is?

A. I do not.

Q. And if you turn to page 3 in your Exhibit F, do you see that -- the shortcut to the same file appearing there again?

A. I do. It's in black because the other files are in green.

Q. Do you know why the same shortcut to that same file keeps showing up in different folders in your Exhibit F?

A. No. I'm not familiar with what that file is.

Page 305

Q. Did you do any analysis to determine whether the MFT modified dates depicted in your Exhibit F can be connected with OneDrive folder synchronization activities?

A. So I'm looking at the folder path of the files, for example, on page -- the first page it says J. Grailer Ecolab and it's not under the OneDrive folder. So it's under the folder path JGrailer Ecolab owns Michael Idium Clinton actually. So it's not under the OneDrive folder.

Q. And that's why you're saying then you didn't do any analysis to see whether the MFT modified dates could be connected with OneDrive folder synchronization activities?

MR. YOSHIMURA: Objection.

BY THE WITNESS:

A. I found no evidence of this artifact being -- or the fact that these multiple files were -- in folders were concurrently accessed at the same time.

Q. Did you do any analysis to determine whether the MFT modified dates in your Exhibit F could be connected to Grailer's activities putting together an e-mail that she sent to her supervisor

Page 306

on January 8th, 2023?

MR. YOSHIMURA: Objection.

BY THE WITNESS:

A. I found no evidence that any of these dates and time changes were a result of e-mail activity by Jessica Grailer.

Q. Did you do an analysis to figure that out one way or the other?

MR. YOSHIMURA: Objection.

BY THE WITNESS:

A. I analyzed the e-mail that she sent because that's specifically looking for any sort of evidence of her e-mailing files to herself and found none.

Q. About how much time did you spend analyzing the files in folders shown in your Exhibit F to determine whether Grailer copied them to her thumb drive?

A. If you're asking me -- so I'm not sure I understand the question.

Q. Well, when did you do the analysis? Did you do this before your February 2023 declaration to determine that the files and folders shown in your Exhibit F were copied to

Page 307

Grailer's thumb drive?

A. So my Exhibit F, your Exhibit 36, my recollection is that I generated this in response to writing a rebuttal to Mr. Pixley's rebuttal to me.

Q. So you performed that analysis then before your second declaration; is that correct?

A. Yes, I believe so. If you're referring to the most -- the last declaration, is that what you're referring to?

So I believe this is -- well, I don't have them all in front of me, so ...

Q. Your supplemental declaration in response to Mr. Pixley was at the end of March 2023.

A. Okay. You could be right. I don't recall the date.

Q. Okay. But the analysis that you performed to conclude that Grailer exfiltrated the files in folders shown in your Exhibit F, which we have marked as Exhibit 36, you believe you performed that analysis before executing that March 2023 declaration, right?

A. My recollection is that I performed

Page 308

this analysis and created this exhibit in response to -- in response to my rebuttal to Mr. Pixley's report.

Q. What is the master file table?

A. Master file table is a Windows system artifact that records when files are created, accessed, modified, or modified on a computer that is running the Windows operating system.

Q. All right. Is the master file table designed to record when files are copied to external storage media?

A. So the Digital Guardian tool is designed to track and record when files are recorded to external USB media. The Windows registry and operating system is not designed to record directly in a discrete location files being copied to an external USB drive.

Q. Okay. An MFT modified date must tell us the date and time when something was modified, right?

A. My understanding is it is the last date that the entry in the master file table was modified.

Q. Okay. So the thing that was modified

Page 309

was the entry in the master file table?

A. Correct, which can be different from the last modified date of an actual file.

Q. Got it. All right.

And does -- in your view, does a change to an MFT modify date relating to a file always mean that a user has accessed that file?

A. I don't know how to answer that question.

Q. You list in your -- the exhibits to your report a lot of cases in which you've testified, right?

A. I do.

Q. Okay. How many cases were you testified -- were you testifying about interpreting outputs from maintenance forensics Axiom software?

A. I would say the majority of them.

Q. Could you tell me the last five?

A. I'd have to have the list of my testimony experience in front of me from my CV to jog my recollection of what the case was about and jog my recollection of what the forensic analysis I performed. They're not all the same.

Page 310

Q. And when did you first receive any certification from Magnet Forensics?

A. Oh, gosh. Maybe 10 years ago. Originally the tool was called Internet Evidence Finder and then that eventually evolved into -- they're calling it Axiom now, but it may be more than ten years.

Q. Okay. And those certifications were provided by the vendor, Magnet Forensics; is that right?

A. Yes.

Q. When did you first get any certification from OSForensics?

A. Oh, gosh. I believe Passmark started offering training and certification for their OSForensics tool several years ago, and so I've passed -- I've been certified on the tool in the past and then I recently, again, trained and recertified in this tool, whatever the date shown in -- as part of one of the exhibits to my CV.

Q. Okay. And that certification was also provided by the vendor OSForensics, correct?

A. The vendor is Passmark, P-A-S-S-M-A-R-K.

Page 311

Q. Thank you.

So Passmark is the developer of OSForensics; is that right?

A. It is.

Q. Okay. Just like Magnet Forensics is the developer of Axiom?

A. Correct.

Q. Thank you for that clarification.

MR. SPLITEK: Let me give you Exhibit 38.

(Deposition Exhibit No. 38 was introduced to the witness.)

BY MR. SPLITEK:

Q. Do you recognize Exhibit 38?

A. I do not. Can I look?

Q. Yes. Take your time.

A. My recollection -- and please correct me if I'm wrong -- is that this report was generated by a special master at the direction of the Judge, but I could be wrong.

Q. Have you reviewed the report marked as Exhibit 38 before?

A. I believe so, yes. If this is the special master report that was brought in, then, yes, I did review that report.

Page 312

Q. And I think the term --

A. What is confusing me is --

Q. The term would be more along the lines of a neutral expert.

A. Okay.

Q. I understand what you mean and you're not off base to use that terminology either.

A. Okay.

Q. So, I mean, did you have an understanding before today that Digital Forensics looked for files on Grailer's iPhone and didn't find them?

A. Yes. Oh, yes. Yes, yes. I'm familiar with this report.

Q. Did you -- do you take any issue with Digital Forensics methods or findings?

A. No.

Q. I thought earlier in the deposition, maybe within the past hour or so, you might have said that Grailer exfiltrated files to her USB thumb drive and/or her iPhone. I'm not trying to mischaracterize what you said. Did I get that right?

Page 313

A. Yes. It's both devices. The forensic evidence shows that both devices were connected to the former work laptop on the evening of January 8th. And I know how to copy -- I can copy files to my iPhone once my iPhone is connected to my laptop.

So it's possible it was the iPhone -- it's possible the files were copied to the iPhone 6S but -- because -- due to the fact that the iPhone 6S was factory reset before it was returned to me by a person that I assume to be Jessica Grailer, I cannot confirm any evidence of activities that occurred on the iPhone 6S.

Q. So you know how to copy Excel spreadsheets and PDFs from a laptop to an iPhone?

A. So when a user plugs in an iPhone to a Windows computer -- I have it configured so that Windows Explorer pops up and you'll see a DCIM folder, which is a digital camera, and it is possible to drop and drag files to that.

But I might have different tools and applications installed on my Windows PC that allows me to do that.

Q. Could an ordinary iPhone user move

Page 314

Excel spreadsheets and PDFs in bulk to an iPhone?

A. I can.

Q. But could an ordinary iPhone user?

A. I don't know if you're saying I'm not ordinary. It's possible.

Q. I'm calling you extraordinary. Take a compliment. I'll tell you, I'm not a witness here. I would have no idea how to bring an Excel spreadsheet or a bunch of Adobe documents into an iPhone.

But you tell me. Could a typical iPhone user do that?

A. So if you plug your iPhone into your laptop, you'll see that Windows will say, hey, do you want to connect this device. You have to hit trust device on it. And it can bring up a Windows -- it can bring up a Windows Explorer entry and you'll see your iPhone there.

And if you click on it, you will see a folder, it will be DCIM, which is digital camera. That is your photographs of -- where your photographs are stored on that phone. You can drop and drag and copy them off and interact with them.

Page 315

It is possible to copy files to that location from your Windows computer.

Q. Not just photos, but also Excel spreadsheets?

A. Anything.

Q. So do you have an opinion, sitting here today, about whether the exfiltration that you claim occurred was to the USB thumb drive or to the iPhone?

A. Because the iPhone 6S was factory reset before it was returned by a person I assume to be Jessica Grailer before it was given to me, that destroyed all evidence, like literally that's just taking all of the documents out of a file cabinet that is the an iPhone, shredding them and burning them.

So no one can state what files existed on that iPhone 6S anymore, or what activities were on there. It is very unfortunate.

The Emtec drive, I've been informed, notwithstanding the fact that the evidence shows that this Emtec drive contained Nalco files, that's without question, it's connected to the laptop on January 8th, 2023, in the evening, I've

Page 316

been informed that Ms. Grailer can no longer find that, that USB drive.

So that would be -- so that's why in my last report my recommendation would be to perform a forensic analysis of this undisclosed computer. Her new Chem Tree work computer, in particular, would be my strong recommendation. That's what I would do if I was working for Chem Tree because I would want to rule out whether that Emtec drive had ever been connected to the new Chem Tree work computer.

If there's no evidence of that, I believe that's very important and relevant to this dispute resolution. That's my opinion.

MR. SPLITEK: Let's go off the record for a moment here.

THE VIDEOGRAPHER: The time is 5:01 p.m. We are going off the record.

(Whereupon, a break was taken, after which the following proceedings were had:)

THE VIDEOGRAPHER: The time is 5:15 p.m. and we are back on the record.

MR. SPLITEK: Mr. Lieb, I have no

Page 317

further questions for you today.

Mr. Yoshimura has an opportunity to ask you questions if he would like, and if he does, I may ask you questions on redirect. But I will turn it over to Mr. Yoshimura.

MR. YOSHIMURA: Thank you, Mr. Splitek. We actually have no questions for Mr. Lieb at this time.

MR. SPLITEK: That's shocking. Then the deposition is over. You can go.

THE WITNESS: Fabulous.

THE VIDEOGRAPHER: The time is 5:15 p.m. This concludes the deposition for today.

Would anybody like a video order and transcript order?

MR. SPLITEK: Yeah, I want both video and the transcript.

MR. YOSHIMURA: I'll take a transcript for now. We'll read and sign.

WITNESS EXCUSED AT 5:15 P.M.

Page 318

IN THE UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WISCONSIN

ECOLAB, INC., and NALCO)
COMPANY, LLC,)
Plaintiffs,)
)
-vs-) No. 3-cv-102-wmc
)
JESSICA GRAILER,)
Defendant.)

I, LAURENCE D. LIEB, being first duly sworn, on oath, say that I am the deponent in the aforesaid deposition, that I have read the foregoing transcript of my deposition taken January 23, 2024, consisting of Pages 1 through 320 inclusive, taken at the aforesaid time and place and that the foregoing is a true and correct transcript of my testimony so given.

Corrections have been submitted
No corrections have been submitted

LAURENCE D. LIEB, Deponent

SUBSCRIBED AND SWORN TO
before me this day
of C.E., 2024.

Notary Public

Page 319

REPORTER'S CERTIFICATE

I, Noreen E. Resendez, Registered Professional Reporter and Notary Public in and for the County of DuPage, State of Illinois, do hereby certify that on the January 23, 2024, the deposition of the witness, LAURENCE D. LIEB, called by the Defendant, was taken before me, reported stenographically and was thereafter reduced to typewriting through computer-aided transcription.

The said witness, LAURENCE D. LIEB, was first duly sworn to tell the truth, the whole truth, and nothing but the truth, and was then examined upon oral interrogatories.

I further certify that the foregoing is a true, accurate and complete record of the questions asked of and answers made by the said witness, at the time and place hereinabove referred to.

The signature of the witness was not waived by agreement.

Pursuant to Rule 30(e) of the Federal Rules of Civil Procedure for the United States District Courts, if deponent fails to read and

Page 320

sign this deposition transcript within 30 days or make other arrangements for reading and signing thereof, this deposition transcript may be used as fully as though signed, and the instant certificate will then evidence such failure to read and sign this deposition transcript as the reason for signature being waived.

The undersigned is not interested in the within case, nor of kin or counsel to any of the parties.

Witness my official signature and seal as Notary Public, in and for DuPage County, Illinois, on this 29th day of January, C.E., 2024.

/s/ Noreen E. Resendez, CSR, RPR, CRR
Notary Public
License No. 084-004182